



Št. naloge: 00497/2010

Datum: 15.02.2010

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **TOMAŽ BARTOL**

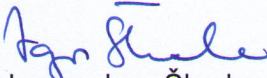
Naslov: **SISTEM PROTIVLOMNEGA VAROVANJA
INTRUDER ALARM SYSTEM**

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija

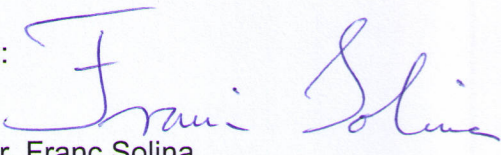
Tematika naloge:

V nalogi predstavite standarda, ki določata lastnosti sistema za javljanje vloma in ropa ter sistema za prenos alarma. Opišite zgradbo in delovanje obeh sistemov ter na praktičnem primeru predstavite načrtovanje, postavitve in konfiguriranje zahtevnejšega alarmnega sistema.

Mentor:


pred. mag. Igor Škraba

Dekan:


prof. dr. Franc Solina



**UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO**

Tomaž Bartol

SISTEM PROTIVLOMNEGA VAROVANJA

DIPLOMSKO DELO NA VISOKOŠOLSKEM STROKOVNEM ŠTUDIJU

MENTOR: pred. mag. Igor Škraba

Ljubljana, 2010

IZJAVA O AVTORSTVU

diplomskega dela

Spodaj podpisani Tomaž Bartol,

z vpisno številko 63030003,

sem avtor diplomskega dela z naslovom:

SISTEM PROTIVLOMNEGA VAROVANJA

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom (naziv, ime in priimek)

pred. mag. Igor Škraba

in somentorstvom (naziv, ime in priimek)

/

- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela
- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki »Dela FRI«.

V Ljubljani, dne 16.06.2010

Podpis avtorja: Tomaž Bartol

ZAHVALA

Najprej bi se zahvalil mentorju, pred. mag. Igorju Škrabi, ki mi je s svojim načinom dela vzbudil veliko zanimanja za snov, ki jo je predaval. Za to ter za vodenje in nasvete pri izdelavi diplomske naloge se mu iskreno zahvaljujem.

Zahvalil bi se tudi sošolcem, saj smo se v času študija skupaj prebijali čez ovire.

Posebna zahvala gre tudi moji bodoči ženi Nataši, ki me je spodbujala pri pisanju in lektoriranju diplomskega dela. Zahvalo pa bi namenil tudi mojemu prvemu otroku, ki bo septembra prišel na svet. Čeprav ga še ni tukaj, mi je na svojevrsten način neskončno pomagal.

Zahvaljujem se tudi Antonu Zidarju za razumevanje in vso podporo v času pisanja diplomskega dela.

Na koncu bi se rad zahvalil še moji družini in družini Šmalc za podporo med študijem.

KAZALO VSEBINE

ZAHVALA.....	II
KAZALO VSEBINE	III
KAZALO SLIK	V
KAZALO TABEL.....	VI
KAZALO TABEL.....	VI
Seznam okrajšav in kratic.....	VII
POVZETEK.....	VIII
ABSTRACT	IX
1. Uvod.....	1
2. Vrste varovanj	2
2.1. Mehansko varovanje (varovanje stanovanj v blokih).....	3
2.2. Elektronsko varovanje (varovanje stanovanjskih hiš)	4
3. Sistem protivlomnega varovanja (protivlomni alarmni sistem).....	5
3.1. Varovanje manj zahtevnih objektov.....	5
3.2. Varovanje srednje zahtevnih objektov.....	6
3.3. Varovanje zahtevnih objektov.....	6
4. Standardi tehničnih sistemov za varovanje.....	7
4.1. Standard SIST EN 50131	7
4.2. Standard SIST EN 50136	9
5. Opis naprav za protivlomno varovanje objektov	12
5.1. Alarmna centrala	12
5.2. Tipkovnica (šifrador)	13
5.3. Senzorji	13
5.3.1. Notranji pasivni infrardeči senzor premika (PIR).....	14
5.3.2. Notranji senzor premika dvojne tehnologije.....	19
5.3.3. Zunanji senzor premika	21
5.3.4. Senzor loma stekla	23
5.3.5. Magnetni kontakti	23
5.3.6. Bariere (žarkovne zapore)	24
5.3.7. Požarni senzorji	24
5.4. Sirena.....	25
6. Primerjava alarmnih naprav proizvajalca DSC in njihovih lastnosti	26
6.1. Komunikacija KEYBUS med napravami	26
6.2. Primerjava alarmnih central proizvajalca DSC	31
6.2.1. Vezalna shema alarmne centrale DSC.....	34
6.3. Primerjava tipkovnic proizvajalca DSC	36
6.4. Primerjava senzorjev proizvajalca DSC.....	39
6.5. Razširitveni modul za dodatnih 8 področij PC5108 proizvajalca DSC	41
6.6. Univerzalni brezžični alarmni komunikator GSM/GPRS GS3055-I proizvajalca DSC.....	43
6.6.1. Zgradba komunikatorja GSM/GPRS GS3055-I.....	44
6.6.2. Povezovalna shema komunikatorja GSM/GPRS GS3055-I	45

6.6.3.	Programiranje komunikatorja	46
7.	Priprava za protivlomni alarmni sistem pri novogradnji	49
8.	Primer izvedbe protivlomnega alarmnega sistema z uporabo naprav proizvajalca DSC	51
8.1.	Napeljava in montaža protivlomnega alarmnega sistema	51
8.1.1.	Zaščita kleti	51
8.1.2.	Zaščita pritličja	53
8.1.3.	Zaščita mansarde	54
8.1.4.	Popis materiala	56
8.1.5.	Vezava senzorjev priključenih na področja (Zx)	57
8.2.	Programiranje protivlomnega alarmnega sistema s pomočjo programskega zapisnika- navodil za uporabo	58
8.2.1.	Podatki o sistemu	59
8.2.2.	Programiranje tipkovnic	59
8.2.3.	Osnovno programiranje sistema	61
8.2.4.	Podrobnejše programiranje sistema	65
8.2.5.	Programiranje področij in particij	67
8.2.6.	Programiranje komunikatorja alarmne centrale	67
8.2.7.	Programiranje izpisov na tipkovnici	69
9.	Zaključek	70
10.	Viri	71

KAZALO SLIK

Slika 1: Shema protivlomnega alarmnega sistema [3].	5
Slika 2: Primer prečkanja osebe mimo aktivnih in pasivnih področij senzorja	15
Slika 3: Primerjava diagramov pokritja senzorja pri širokokotni in ozkokotni različici.	16
Slika 4: Diagram pokritja senzorja pri 360 ^o različici s tremi lečami.	16
Slika 5: Pravilna postavitev notranjega infrardečega senzorja premika med dvema oknom [8].	19
Slika 6: Primer delovanja senzorja sestavljenega iz dveh IR elementov [8].	21
Slika 7: Možni lažni alarm zaradi premikanja dreves [8].	22
Slika 8: Nepravilno usmerjanje senzorja (levo) ter pravilna usmeritev senzorja v objekt (desno) [8].	23
Slika 9: Možna postavitev senzorjev loma stekla [8].	23
Slika 10: Primer sprejemnika in oddajnika bariere	24
Slika 11: Izbira pozicij požarnih senzorjev za minimalno in boljšo zaščito [3].	25
Slika 12: Izgled zunanjih siren.	25
Slika 13: Primer prevelike razdalje kabla med alarmno centralo in modulom C [12].	26
Slika 14: Prikaz stanja START (S) in STOP (P) [13].	28
Slika 15: Podrejena naprava zadrži SCL linijo, ker je zasedena [13].	28
Slika 16: Primer sprejemanja/pošiljanja dveh bajtov podatkov [13].	29
Slika 17: Primer potrditvenega signala ACK sprejemnika [13].	29
Slika 18: Primer pisanja nadrejene naprave v podrejeno [13].	30
Slika 19: Primer branja nadrejene naprave iz podrejene [13].	30
Slika 20: Priključki centrale PC1616 / 1832 / 1864 [6].	35
Slika 21: Zunanja oblika tipkovnice LCD PK5500 [11].	36
Slika 22: Tipkovnica LCD ICON PK5501 (levo) in tipkovnica LED PK5516, (desno) [16].	37
Slika 23: Notranji infrardeči senzor premika LC-100PI (levo) in diagram pokritja (desno) [11].	39
Slika 24: Zunanja oblika senzorjev loma stekla Acuity proizvajalca DSC [11].	40
Slika 25: Simulator loma stekla AFT-100.	41
Slika 26: Notranja shema modula PC5108 za povečanje področij sistema [12].	42
Slika 27: Zgradba komunikatorja GSM/GPRS GS3055-I proizvajalca DSC [15].	44
Slika 28: Povezovalna shema komunikatorja GSM/GPRS GS3055-I proizvajalca DSC [15].	45
Slika 29: Pregled telefonske strani v programskem vmesniku GS3055.	46
Slika 30: Imenik kratkih sporočil v programskem vmesniku GS3055 (SMS dialler page).	47
Slika 31: Imenik izhodov v programskem vmesniku GS3055 (Outputs page).	47
Slika 32: Siva cev RFS (levo) in oranžna cev RBT (desno) velikosti $\Phi 16$ [16].	49
Slika 33: Kabel Licy za povezavo med alarmno centralo in ostalimi napravami [16].	50
Slika 34: Tloris kleti z legendo protivlomnih simbolov.	52
Slika 35: Tloris pritličja z legendo protivlomnih simbolov.	53
Slika 36: Tloris mansarde z legendo protivlomnih simbolov.	55
Slika 37: Pregled povezav alarmne centrale in razširitvenih vmesnikov (modulov).	56
Slika 38: Primer vezave SEOL v z NC stikalom (levo) in NO stikalom (desno).	57
Slika 39: Primer vezave DEOL (levo) in vezave DEOL s sabotažnim stikalom (desno).	58

KAZALO TABEL

Tabela 1: Primerjava zahteve glede napajanja sistema v različnih varnostnih razredi [5].....	9
Tabela 2: Klasifikacija alarmnih prenosnih sistemov po času prenosa [2].	10
Tabela 3: Klasifikacija alarmnih prenosnih sistemov po največjem dovoljenem času prenosa [2].....	10
Tabela 4: Klasifikacija alarmnih prenosnih sistemov po času sporočila o napaki [2].	10
Tabela 5: Klasifikacija alarmnih prenosnih sistemov po razpoložljivosti [2].	11
Tabela 6: Jakost električnega polja (E) oddaljenosti 30 cm od naprav [9].	17
Tabela 7: Vrednosti magnetnega polja (B) od različnih oddaljenosti od naprav [9].	18
Tabela 8: Opis standarda zaščite IP [10].....	22
Tabela 9: Primerjava alarmnih central serije Power pri proizvajalcu DSC [12].	31
Tabela 10: Primerjava alarmnih central serije New power pri proizvajalcu DSC [11].....	32
Tabela 11: Primerjava tipkovnic glede na prikaz stanja.	38
Tabela 12: Primerjava lastnosti tipkovnic serije New Power pri DSC [11].	39
Tabela 13: Notranja shema modula PC5108 za razširitev sistema [12].	42
Tabela 14: Popis materiala za omenjen objekt.	57
Tabela 15: Veljavni vnosi za funkcijske tipke [12].	60
Tabela 16: Možni vnosi področij [12].	61
Tabela 17: Možni vnosi za izhode PGM.....	63
Tabela 18: Opis 12 lastnosti, ki jih lahko definiramo za vsako področje.....	66
Tabela 19: Komunikacijski formati za prenos alarma.....	68

Seznam okrajšav in kratic

AC	<i>Alternating current</i>	Izmenični tok
AWG	<i>American Wire Gauge</i>	Standardna tabela debelin žice
DC	<i>Direct current</i>	Enosmerni tok
DEOL	<i>Double End Of Line</i>	Dvojni zaključni upor
DTMF	<i>Dual Tone Multi-Frequency</i>	Način TK signalizacije
EMI	<i>Electromagnetic Interference</i>	Elektromagnetne motnje
EMS		Elektromagnetno sevanje
FTC	<i>Fail To Cumunicate</i>	Napaka povezave telefonske linije
IC	<i>Integrated Circuit</i>	Integrirano vezje
I2C	<i>Inter-Integrated Circuit</i>	Serijsko vodilo
LCD	<i>Liquid Cristal Display</i>	Prikazovalnik na tekoče kristale
NC	<i>Normally Closed Contact</i>	Normalno zaprt kontakt
NO	<i>Normally Off Contact</i>	Normalno zaprt kontakt
PIR	<i>Passive infrared sensor</i>	Pasivni infrardeči senzor
PSTN	<i>Public Switched Telephone Network</i>	Omrežje za telefonske storitve
RFI	<i>Radio Frequency Interference</i>	Radiofrekvenčne motnje
SEOL	<i>Single End Of Line</i>	Enojni zaključni upor
SIA	<i>Security Industry Association</i>	Združenje proizvajalcev varnostne
opreme		
SMS	<i>Short Message Service</i>	Tekstovna kratka sporočila
TLM	<i>Telephone Line Monitoring</i>	Preverjanje delovanja telefonske linije

POVZETEK

Tema diplomske naloge je predstavitev sistema protivlomnega varovanja in primer vgradnje sistema v stanovanjsko hišo.

V prvem delu sem opisal vrste varovanj, ki jih nudijo varnostne službe v Sloveniji. Poleg fizičnega in tehničnega varovanja, imamo na razpolago tudi kombinacijo obeh varovanj. Sistem protivlomnega varovanja je primer enega od tehničnih varovanj. Varovanje lahko delimo tudi na mehansko ali elektronsko varovanje.

V drugem delu je opisan sistem protivlomnega varovanja ter opis varovanja objektov, ki se delijo po zahtevnosti. V naslednjem poglavju sta opisana standarda SIST EN 50131 in SIST EN 50136, ki določata lastnosti protivlomnega alarmnega sistema in časovne zahteve pri prenosu alarmnih sporočil.

V tretjem delu sem predstavil vse pomembne naprave, ki sestavljajo sistem protivlomnega varovanja. Te naprave so: alarmna centrala, tipkovnica, senzorji in sirena. Posebno pozornost sem namenil senzorjema PIR in MW ter sestavi in delovanju obeh.

V četrtem delu so predstavljene alarmne naprave proizvajalca DSC, njihova medsebojna primerjava ter komuniciranje naprav med seboj. Za komunikacijo je uporabljeno vodilo in protokol I²C. Naj tukaj omenim še univerzalni brezžični komunikator GSM/GPRS GS3055-I, ki deluje v omrežju GSM. Zagotavlja nam dodaten način komunikacije v primeru, ko telefonske linije nimamo na razpolago ali v primeru prekinjene linije.

V petem delu je predstavljen primer vgradnje protivlomnega alarmnega sistema z napravami proizvajalca DSC. S programom AutoCAD Electrical 2009 sem izdelal načrt posameznih nadstropij z vrisanimi protivlomnimi elementi. Zatem pa sem opisal pomembnejše nastavitve pri programiranju sistema, ki ga nastavljamo preko tipkovnice.

Ključne besede: tehnično varovanje, sistem protivlomnega varovanja, alarmna centrala, tipkovnica, senzor PIR&MW, standard SIST EN 50131 in SIST EN 50136, protokol I²C.

ABSTRACT

The theme of this thesis is the presentation of the intruder alarm system and installation of such system in residential building.

In the first part I described the different types of security, which are offered in security services in Slovenia. In addition to the physical and technical security, there is also available a combination of both. Intruder alarm system is an example of one of the technical protection. Protection can also be classified in physical or electronic security.

The second part describes the intruder alarm system and a description of security installations, which are divided according to the complexity. The next chapter describes the SISTE EN 50131 and SIST EN 50136 standard, which determine the properties of intruder alarm system and time requirements for transmission of alarm messages.

In the third part I presented all the important devices which composed the intruder alarm system. These devices are: alarm control panel, keypad, sensors and siren. I devoted special attention to PIR and MW sensor and the composition and functionality of both.

In the fourth part I presented the alarm devices of the DSC manufacturer, their mutual comparison and communication between them. For communication the I²C bus and protocol is used. Here we can mention the GSM/GPRS GS3055-I universal wireless communicator which operates in GSM network. It provides us an additional way of communication where telephone lines are not available or in case of broken lines.

In the fifth part I presented the example of installation of intruder alarm system with devices of DSC manufacturer. With AutoCAD Electrical 2009 I have made plans for the individual floor with elements of intrusion. Then I described the important programming settings of the alarm system which can be set up with keypad.

Keywords: technical security, intruder alarm system, alarm control panel, keypad, PIR&MW sensor, SIST EN 50131 and SIST EN 50136 standard, I²C protocol.

1. Uvod

Ko sem izbiral temo za diplomsko nalogo, sem takoj vedel, da se bo ta dotikala gradnje elektroinštalacij ter raziskovanja udobja in varnosti stanovanjskih objektov. Vsekakor si nekoč želim sam ustvariti dom in pri tem projektirati načrt električnih instalacij, električne opreme in vgradnjo naprednejšega sistema, da bi lahko le ta deloval kot pameten dom. Pameten dom naj bi bil prijeten in tehnološko visoko napreden, v katerem bi lahko preprosto upravljali s hišno razsvetljavo, ogrevanjem, hišnim kinom, zavesami in navsezadnje z vsem kar si zaželiš. Poleg tega se želim naučiti več o varnostnih sistemih, vseh napravah in senzorjih, ki jih lahko vgradimo v svoje stanovanje. Glavna tema mojega diplomskega dela se dotika ravno protivlomnega alarmnega sistema.

Število vlomov in tatvin narašča. To je privedlo do večjega povpraševanja po varnostnih sistemih, s katerimi bi lahko učinkovito zavarovali sebe in naše imetje. Vse več ljudi se odloča za vgradnjo protivlomnega sistema, požarnega sistema, video-nadzornega sistema, kontrole pristopa ali drugih varovanj. Varnost je ena od najpomembnejših vrednot vsakega človeka, vendar se tega zavemo šele takrat, ko gre kaj narobe.

Sistem protivlomnega varovanja je najpogostejši sistem varovanja pri nas. Zato sem se v tej nalogi osredotočil predvsem na to. Kot praktičen primer sem postavil protivlomni alarmni sistem v hiši, od priprave pri novogradnji pa do vzpostavitve alarmnega sistema.

2. Vrste varovanj

Ko zapustimo svoje domove za več tednov, moramo poskrbeti za varnost svojega premoženja. Svoj dom lahko preventivno zavarujemo z naslednjimi preprostimi ukrepi [1]:

- Doma ne hranimo večje vsote denarja, rešitev je tudi bančni sef.
- Rolete na oknih naj bodo spuščene, saj bo tako vlomilec mislil, da smo doma.
- Poštni nabiralnik naj bo prazen, naj nam ga izpraznijo sorodniki ali sosedje.
- Ključev od vhodnih vrat ne puščamo na znanih skrivališčih (pod predpražnikom, pod rožo).
- Na vratih ne puščamo obvestil, da nas ni doma.
- S pomočjo avtomata za prižiganje luči pustimo kakšno luč goreti v določenem delu hiše.
- Pred odhodom uredimo okolico in jo ne pustimo razmetano, kot da nas ni že dolgo doma.
- Odstranimo vse orodje in lestve s katerimi bi vlomilec lažje dostopal do oziroma v objekt.
- Sosede obvestimo o tem, da smo na dopustu in naj bodo bolj pozorni na morebitne vlomilce.
- Osvetlimo okolico hiše, saj vlomilci neradi delajo v svetlem.

Na začetku so bila varovanja fizična, s prisotnostjo treniranih in izobraženih ljudi. Nato se je potreba po varovanju povečevala, saj se je človek začel ukvarjati z mislijo, kako bi varovanje postavil brez prisotnosti človeka. Začeli so z varovalnimi ograjami opremljenimi s stvarmi, ki so ustvarjale hrup. Tako prisotnost ljudi ni bila več potrebna in ta namembnost se je razširjala ter izpopolnjevala do današnjih dni.

Za zagotovitev kvalitetnega varovanja je potrebno skrbno strokovno načrtovanje in pravilna izbira sredstev in naprav, ki jih bomo uporabili. Določiti je treba stopnjo ogroženosti človeških življenj in materialnih dobrin. Določiti moramo verjetna mesta za morebitne poskuse nepooblaščenih vdorov v objekt, pravilno postavitev naprav ter javljalnikov. Učinkovitost varovanja je odvisna tudi od hitrega odziva dežurne in servisne službe.

Varovanje za naročnika je lahko dobra ekonomska poteza in ne samo strošek vgradnje sistema. Stroški investicije za tehnično varovanje so lahko precej nižji kot stroški morebitne škode ob vlomu, kraji, požaru ter podobnem. Zelo pomembna je kakovost vgrajenih tehničnih sredstev v sistem varovanja. Tako lahko zmanjšamo verjetnost lažnih alarmov, ki so nezaželeni tako pri uporabniku kot pri varnostnih službah.

Področje varovanja delimo na tri glavna podpodročja [2]:

- FIZIČNO VAROVANJE,
- TEHNIČNO VAROVANJE in
- FIZIČNO – TEHNIČNO VAROVANJE, ki je kombinacija obeh.

V nadaljevanju se bomo omejili na tehnično varovanje s protivlomnim varovanjem. Tehnično varovanje pomeni varovanje ljudi in njihove lastnine z uporabo sistemov tehničnega varovanja. Sistemi tehničnega varovanja se delijo na šest večjih skupin [2]:

- SISTEM MEHANSKE ZAŠČITE,
- SISTEM PROTIVLOMNEGA VAROVANA,
- SISTEM PROTIPOŽARNEGA VAROVANJA,
- SISTEM VIDEO NADZORA,
- SISTEM PRISTOPNE KONTROLE in
- SISTEMI ZA DETEKCIJSKO MERJENJE EKSPLOZIVNIH PLINOV IN DRUGI TEHNIČNI ALARMI.

Posamezne skupine lahko med seboj kombiniramo in združujemo. Sistem tehničnega varovanja, ki alarmna sporočila prenaša na daljavo, razdelimo na tri ločene segmente [2]:

- alarmni sistem varovanega objekta, ki signalizira stanje sistema. Signalizacija je lahko izvedena lokalno ali na daljavo do varnostnega nadzornega centra (VNC).
- sistem za prenos alarma, ki opravlja funkcijo prenosa alarmnih sporočil do oddaljenega VNC-ja. Alarmna sporočila se prenašajo po prenosnem omrežju. Najbolj razširjeno je telefonsko omrežje, ki nudi več različnih možnosti prenosa.
- varnostni nadzorni center (VNC), ki je informacijsko središče sistema tehničnega varovanja. VNC sprejema alarmna sporočila iz vseh objektov ter jih obdeluje, prikazuje in arhivira. Osebe v sprejemnem centru obvešča ustrezne intervencijske službe za nadaljnje ukrepe.

2.1. Mehansko varovanje (varovanje stanovanj v blokih)

Prvi in najosnovnejši ukrep pri zaščiti našega doma je mehanska zaščita. Je prva ovira za osebo, ki namerava storiti kaznivo dejanje. Mehansko varovanje je namenjeno opozarjanju na varovan prostor in preprečuje vstop nepooblaščenim osebam. Vrata v stanovanju so opremljena s ključavnicami z jeklenimi vložki. Šibka vrata se dodatno zavarujejo z varnostno verigo, kukalo v vratih pa nam omogoča popolno preglednost. Okna varujemo s kljukami s cilindričnimi vložki ali jih zaščitimo z rešetko, pritrjeno na okvir. Stekla lahko dodatno prelepimo z varnostno folijo [1]. Protivlomne folije preprečujejo lomljenje steklenih površin. Ob udarcu se steklo razbije, vendar pa ne razpade zaradi nalepljene folije. Protivlomne omare, trezorje in blagajne lahko uporabimo za shranjevanje tajnih dokumentov ali stvari, ki so nam pomembnejše.

Vse omenjene varovalne naprave pomenijo za vlomilca le oviro. Zadržijo ga le toliko časa, da jih obvlada ali razbije. S tem časom se tudi meri uspešnost mehanske zaščite. Dlje ko bomo zadrževali nepooblaščen osebe pred vlomom, boljša je naša zaščita. Mehanski zaščiti se danes daje premajhen pomen, saj marsikdaj opazimo povsem neprimerna vhodna vrata, navadne ključavnice, velika nezaščiten izložbena okna, lahko dostopnost do vlomilnih točk in slabo zunanjo osvetljenost. Dovolj velik problem mehanske zaščite je tudi videz, saj marsikje zaradi zahtev arhitektov in estetike le ta ni možna.

Okoli 75 % vlomov se zgodi skozi vhodna vrata. V višjih nadstropjih je dostop v stanovanje možen samo skozi vhodna vrata. Tatovi in vlomilci imajo radi lahko delo. Zaradi tega moramo poskrbeti za tehnične ovire, ki bodo vlom onemogočile ali ga upočasnile in naredile hrupnega. To bo pritegnilo pozornost sosedov ali naključnih mimoidočih, ter vlomilca odgnalo.

Varnostna vrata ali protivlomna vrata so najbolj učinkovita zaščita dostopa v objekt, ki že v osnovni izvedbi vsebujejo vse mehanske varovalne elemente, kot so močna konstrukcija, različne zapore, ki varujejo vrata pred snemanjem s tečajev, varne cilindrične vložke, varnostna okovja in podobno. Takšna vrata imetniku torej zagotavljajo in nudijo več vrst zaščite. Protivlomna zaščita varuje pred lomljenjem vrat, lomljenjem cilindričnega vložka, vrtanjem in snemanjem vrat s tečajev. Nekatera varnostna vrata nudijo tudi zaščito pred ognjem. Zaradi same protivlomne in ognjevarne zaščite pa takšna vrata imetniku zagotavljajo tudi zaščito pred hrupom in dimom. Ekonomsko gledano je ta zaščita najbolj primerna.

Seveda v današnjem svetu to ni dovolj. Če je objekt zavarovan samo mehansko, je verjetnost za vlom večja. Zavedati se moramo, da nam alarmni sistem samo javlja vlom in ne prepreči vlomilcu vstop v stanovanje [1].

2.2. Elektronsko varovanje (varovanje stanovanjskih hiš)

Kombinacija mehanskega in elektronskega varovanja je učinkovitejša za preprečevanje vlomov. Če smo v mehanskem varovanju podali primer zaščite stanovanja v višjem nadstropju, se lahko tukaj omejimo na zaščito stanovanj v nižjih nadstropjih in stanovanjskih hiš. Tukaj je vstop možen na več mestih. Nič nam ne pomaga, če optimalno zaščitimo vhodna in stranska vrata, ko pa imamo lahko dostopna okna. Ravno zaradi tega se filozofija varovanja stanovanjskih hiš nagiba k tehničnemu varovanju z alarmnimi napravami. Tukaj ne preprečujemo dostopa v objekt, ampak vstop v varovane prostore zaznavamo in ustrezno javljamo. Rečemo lahko tudi, da je bil sprožen alarm. Javljanje je lahko lokalno s pomočjo sirene ali bliskavice, alarm pa lahko prenesemo tudi v varnostno nadzorni center (VNC) podjetja za varovanje. Od VNC-ja lahko pričakujemo takojšnjo intervencijo ustrezno usposobljenih in opremljenih varnostnikov [1].

Med elektronske sisteme varovanja štejemo tehnična varovanja brez mehanske zaščite:

- sistemi nadzora gibanja (identifikacija, sistem pristopne kontrole),
- alarmni sistemi (sistem protivlomnega varovanja, sistem protipožarnega varovanja, sistem video nadzora, ostali tehnični alarmi).

3. Sistem protivlomnega varovanja (protivlomni alarmni sistem)

Med vsemi primeri varovanja je protivlomni alarmni sistem najbolj razširjena oblika varovanja pred nepooblaščenim vstopom. S pomočjo javljalnikov se odkriva gibajoče objekte znotraj varovanega področja na osnovi različnih fizikalnih pojavov. Sistem nas v primeru vloma opozori z zvočnimi ali s svetlobnimi signali. Javljanje vloma ima tudi funkcijo tihega alarma, kjer se alarm prenese preko telefonske linije v VNC. Vsak protivlomni alarmni sistem sestavljajo naslednji elementi:

- alarmna centrala,
- senzorji (javljalniki),
- tipkovnica (šifrator),
- stikalo za klic v sili (panik tipka),
- sirena (notranja in/ali zunanja),
- telefonski pozivnik.



Slika 1: Shema protivlomnega alarmnega sistema [3].

S takšno shemo (slika 1) lahko ponazorimo večino alarmnih sistemov. Od vrste objekta, stopnje varovanja ter od želje in potreb naročnika je odvisno, koliko in katere elemente varovanja bomo vgradili.

Kakšen alarm potrebujemo je odvisno od njegove namembnosti. V varnostnih službah se objekte glede na varnostno ogroženost deli na tri nivoje [4]:

- varnostno manj zahtevni objekti,
- srednje zahtevni objekti in
- zelo zahtevni objekti.

3.1. Varovanje manj zahtevnih objektov

V varnostno manj zahtevne objekte štejemo stanovanje, hiše, manjše in večje lokale, trgovine, manjša skladišča, garaže, itn. Alarmni sistemi, ki zadovoljujejo tako stopnjo varnosti, so manj zmogljivi vendar enako kvalitetni. Alarmna centrala naj omogoča priklop vsaj 6 alarmnih

elementov in povezavo z nadzornim centrom. Tipkovnica naj bo opremljena z led diodami za kontrolo delovanja alarmnega sistema. Omogoča naj tudi vgradnjo telefonskega odzivnika za obveščanje na mobilni telefon uporabnika.

Senzorji naj bodo postavljeni v vse pomembnejše prostore, predvsem na hodnike in stopnišča. Vsi senzorji so lahko tipa PIR (Pasivni infrardeči senzor). Vhodna vrata naj bodo opremljena z magnetnim kontaktom. Sistem pa naj bo priklopljen na nadzorni center, kjer bo varnostna služba v primeru sproženega alarma ustrezno posredovala [4].

3.2. Varovanje srednje zahtevnih objektov

Srednje zahtevni objekti so manjše tovarne, skladišča, šole, trgovine, itn. V teh primerih moramo uporabiti zmogljivejšo alarmno centralo. Omogočati mora razširljivost za večje število senzorjev, možnost priklopa relejnih modulov za krmiljenje vrat, zapahov, zapiranje oken itn. Imeti mora možnost kontroliranja telefonske linije vsaj vsakih 24 ur. Omogočati mora uporabo večjega števila kod za uporabnike. Tipkovnica naj bo opremljena z LCD prikazovalnikom za boljšo komunikacijo z uporabniki. Ima naj možnost daljinskega nadzora. Senzorji, ki jih uporabljamo v takšnih objektih, naj bodo kakovostni. Uporabijo naj se kombinirani PIR in mikrovalovni senzorji, za bolj zanesljivo varovanje brez lažnih alarmov. Vrata naj bodo opremljena z magnetnimi kontakti, okolica objekta pa naj bo varovana s senzorskim kablom ali žarkovnimi zaporami (barierami) [4].

3.3. Varovanje zahtevnih objektov

Zahtevni objekti so velike tovarne, banke, nakupovalni centri, menjalnice, državne institucije, muzeji, itn. Alarmni sistem mora v teh primerih omogočati vse kar je bilo naštet pri varovanju srednje zahtevnih objektov. Poleg tega pa mora alarmni sistem omogočati še povezavo s sistemi vstopne kontrole, videonadzornimi sistemi in integracijo s sistemom fizičnega varovanja (receptorska služba, varnostni nadzorni center). Povezava z varnostnim nadzornim centrom mora biti izvedena tako, da omogoča kontrolo telefonske linije, dodatno povezavo z internetom z nadzirano linijo ali priklop dodatnega modula GSM za brezžično telefonsko povezavo. Dostop do telefonske linije je žal mnogokrat zelo enostaven in velikokrat pride do prekinitve že pred samim vlomom.

Prav tako pa so potrebni redni obhodi intervencijske službe. Varnostniki ali receptorji, zaposleni v takšnem objektu, naj bi bili strokovno ustrezno usposobljeni, z najmanj V. stopnjo zahtevnosti izobrazbe in ustreznimi delovnimi izkušnjami [4].

4. Standardi tehničnih sistemov za varovanje

Po definiciji je standardizacija dejavnost vzpostavljanja določil, glede na dejanske ali možne težave za skupno in ponavljajočo se uporabo z namenom, da se doseže optimalna stopnja urejenosti na danem področju. Standard pa je dokument, ki nastane s konsenzom in ga odobri priznani organ.

Slovenski inštitut za standardizacijo (SIST) vključuje vrsto standardov, ki določajo lastnosti in način namestitve tehničnih sistemov za varovanje. Opisali bomo standard SIST EN 50131 in standard SIST EN 50136, ki določata lastnosti protivlomnega alarmnega sistema in prenos alarmnih sporočil.

4.1. Standard SIST EN 50131

Standard SIST EN 50131 določa lastnosti protivlomnega alarmnega sistema (**Sistem za javljanje vloma in rop** – ang. *Intrusion and hold-up systems*). Glede na prejšnje standarde ta standard prinaša ogromno izboljšav in bo odgovoril na marsikatero nejasnost pri projektiranju, vgradnji in vzdrževanju protivlomnih sistemov.

Standard SIST EN 50131 je namenjen poenotenju protivlomnih standardov v Evropski uniji. Prvi deli standarda so bili napisani že v začetku 90-ih let, ko je zaživela želja po enotni evropski standardizaciji na področju protivlomnega varovanja. Različni deli standarda so bili do danes že revidirani, nekateri pa napisani na novo. V letu 2007 so bili praktično vsi deli standarda prenovljeni. Danes ima standard EN50131 osem delov [6]:

- 1) EN 50131-1: Osnovne (sistemske) zahteve,
- 2) EN 50131-2-2: Zahteve za pasivne infrardeče javljalnike,
EN 50131-2-3: Zahteve za mikrovalovne javljalnike,
EN 50131-2-4: Zahteve za kombinirane pasivne infrardeče in mikrovalovne javljalnike,
EN 50131-2-5: Zahteve za kombinirane pasivne infrardeče in ultrazvočne javljalnike,
EN 50131-2-6: Zahteve za kontaktne javljalnike (magnetne),
EN 50131-2-7-1: Zahteve za javljalnike vloma – javljalniki loma stekla (akustični),
EN 50131-2-7-2: Zahteve za javljalnike vloma – javljalniki loma stekla (pasivni),
EN 50131-2-7-3: Zahteve za javljalnike vloma – javljalniki loma stekla (aktivni),
- 3) EN 50131-3: Oprema za kontrolo in indikacijo,
- 4) EN 50131-4: Opozorilne naprave,
- 5) EN 50131-5-3: Zahteve za povezovalno opremo, ki uporablja radio-frekvenčno tehniko,
- 6) EN 50131-6: Napajalne enote,
- 7) EN 50131-7: Navodila za uporabo,
- 8) EN 50131-8: Sistemi in naprave z varnostno meglo.

Pomemben je predvsem prvi del EN 50131-1, ki razvršča protivlomne alarmne sisteme v štiri varnostne razrede. Prvi varnostni razred pomeni najnižjo stopnjo varovanja, štiri pa najvišjo. Z razvrščanjem sistemov določimo obseg sistema, signalizacijo in varnost sistema [5]:

- varnostni razred 1 – majhno tveganje, za vlomilca se pričakuje malo znanja o protivlomnih sistemih in uporabo enostavnih orodij, ki so lahko dosegljiva.
- varnostni razred 2 – majhno do srednje tveganje, za vlomilca se pričakuje omejeno znanje o protivlomnih sistemih in uporabo več vrst osnovnih orodij.
- varnostni razred 3 – srednje do visoko tveganje, za vlomilca se pričakuje, da je dobro seznanjen s protivlomnimi sistemi in ima dostop do vsestranskega spektra orodij.
- varnostni razred 4 – visoko tveganje, kjer ima varnost prednost pred vsemi drugimi dejavniki. Na tej ravni se od vlomilca pričakuje, da ima sposobnost in vire za načrtovanje vdora skupaj s posebno opremo, ki jo uporablja.

Na določitev varnostnega razreda vplivajo tehnična oprema protivlomnega alarmnega sistema na samem objektu, prenosne poti do VNC-ja in sam VNC. Za varnostni razred 3 morajo npr. senzorji uporabljati "antimasking" tehnologijo, ki zagotavlja zaščito senzorja pred nezaželenim približevanjem in prekrivanjem senzorja. Prikrita zaščitna stikala naprav (tamper stikala) so obvezna v vseh varnostnih razredih razen v prvem.

Prvi del standarda določa tudi razvrstitev opreme. Za razvrstitev opreme obstajajo štiri skupine naprav, ki so razvrščene glede na okolje delovanja [6]:

- skupina 1 – notranje naprave (Indoors controlled), ki so primerne za vgradnjo v stanovanjske hiše in pisarne. Temperatura je nadzorovana od +5 °C do +40 °C in do 75 % relativne vlažnosti.
- skupina 2 – notranje naprave v splošnem (Indoors uncontrolled), ki so primerne za vgradnjo v trgovinah, restavracijah in skladiščih. Temperatura je nadzorovana od +10 °C do +40 °C, povprečna relativna vlažnost je 75 %, brez kondenzacije.
- skupina 3 – zunanje naprave (Outdoors sheltered), ki so zaščitene pred direktnim vplivom sonca in dežja. Temperatura je nadzorovana od -25 °C do +50 °C, povprečna relativna vlažnost je 75 %, brez kondenzacije.
- skupina 4 – zunanje naprave v splošnem (Outdoors exposed), ki so izpostavljene vremenskim vplivom. Temperatura je nadzorovana od -25 °C do +60 °C, povprečna relativna vlažnost je 95 %.

Sistemi se razlikujejo tudi v pogostosti vzdrževanj. Glede na stopnjo varnostnega razreda bo število vzdrževanj enako:

- Varnostni razred 1: 1x letni pregled sistema.
- Varnostni razred 2 in 3: 2x letni pregled sistema ali 1x letni in 1x daljinski pregled.
- Varnostni razred 4: 2x letni pregled sistema.

Standard določa tudi zahteve glede napajanja sistema v mirovanju v odvisnosti od varnostnega razreda. V tabeli 1 vidimo koliko časa mora sistem delovati izključno na baterije.

TIP A podaja varovanje sistema z baterijami, ki jih lahko ponovno napolnimo (rechargeable batteries), TIP B pa uporabo baterij brez ponovnih polnjenj.

Vrsta oskrbe z električno energijo	Varnostni razred 1 (ure)	Varnostni razred 2 (ure)	Varnostni razred 3 (ure)	Varnostni razred 4 (ure)
TIP A	12	12	24	24
TIP B	24	24	120	120

Tabela 1: Primerjava zahteve glede napajanja sistema v različnih varnostnih razredih [5].

Posamezne institucije se že prilagajajo in podajajo svoje zahteve glede varnostnih standardov. Združenje bank Slovenije pripravlja minimalne zahteve in priporočila za varovanje bank in bančnega poslovanja. Banka bo od izvajalca sistema tehničnega varovanja zahtevala, da poda izjavo o skladnosti z ustreznimi standardi za celoten sistem. Minimalni dovoljeni razred za banko po standardu EN 50131-1 je razred 2. Najbolj vitalni in varnostno izpostavljeni bančni objekti (npr. centralni trezor) pa bodo najmanj razreda 3 ali celo 4.

4.2. Standard SIST EN 50136

Standard opisuje sisteme in opremo za prenos alarma (**Alarmni sistemi: Sistemi in oprema za prenos alarma** – ang. *Alarm systems: Alarm transmission systems and equipment*). Standard v prvem delu (SIST EN 50136-1-1) istočasno s podajanjem sistemskih zahtev, v nekaterih členih podaja tudi klasifikacijo sistemov za prenos alarmov. V drugem delu (SIST EN 50136-2-1) standard določa zahteve za opremo, ki sestavlja sistem za prenos alarma.

Poglavitna naloga sistema za prenos alarma je hiter in verodostojen prenos alarmnih sporočil z varovanega objekta do alarmnega sprejemnega centra. Evropska oziroma mednarodna standardizacija opredeljuje zahteve za sisteme za prenos alarma v seriji evropskih standardov EN 50136, ter serij mednarodnih standardov IEC 839-5. Splošne zahteve za alarmne prenosne sisteme so v obeh skupinah standardov podobne, vendar evropski standardi postavljajo nekoliko ostrejša zahteve, ki jih tudi natančno opredeljujejo [2].

Klasifikacija sistemov za prenos alarma se vrši po več kriterijih, in sicer odvisno od namembnosti alarmnega sistema varovanega objekta (protivlomni, protipožarni ali sistem pristopne kontrole), ki je preko sistema za prenos alarma povezan z VNC-jem. Standard razlikuje med štirimi klasifikacijami. Vsaka klasifikacija je razdeljena na razrede, ki določajo ali je sistem bolj ali manj zanesljiv [2].

KLASIFIKACIJA PO ČASU PRENOSA

Čas prenosa (D-transmission time) je definiran od trenutka spremembe stanja na vmesniku oddajnika, ki je del alarmnega sistema varovanega objekta, do trenutka, ko je v centru za sprejem alarmov spremenjeno stanje zaznal vmesnik sprejemnika. Po času prenosa alarmnih sporočil se alarmni sistemi razvrščajo v pet razredov opisanih v tabeli 2.

Klasifikacija v razrede je določena s povprečno aritmetično sredino časa vseh prenosov ali z povprečnimi izmerjenimi časi za 95 % vseh prenosov, ki ne bi smeli presežati vrednosti v

tabeli 2. Zahteve za klasifikacijo po času prenosa, ki jih prikazuje tabela 2, veljajo za vse vrste alarmnih sporočil, ki se prenašajo po istem alarmnem prenosnem sistemu v normalnem oziroma stabilnem režimu obratovanja. V primeru izpada notranje povezave med alarmnim sistemom varovanega objekta in sistemom za prenos alarmov, mora alarmni prenosni sistem generirati alarmno sporočilo ali pa sporočilo o napaki, ki bi se moralo prenesti do centra za sprejem alarmov.

RAZRED	D0 [s]	D1 [s]	D2 [s]	D3 [s]	D4 [s]
Aritmetična sredina časov vseh prenosov	Ni zahtev	120	60	20	10
Izmerjeni časi za 95% vseh prenosov	240	240	80	30	15

Tabela 2: Klasifikacija alarmnih prenosnih sistemov po času prenosa [2].

KLASIFIKACIJA PO NAJVEČJEM DOVOLJENEM ČASU PRENOSA

Poleg klasifikacije po času prenosa se uporablja tudi klasifikacija po največjem dovoljenem času prenosa (M-maximum acceptable transmission time). Ta prav tako velja za vsa alarmna sporočila, ki jih prenaša sistem za prenos alarmov. Za razliko od prejšnje klasifikacije po času prenosa so tukaj največji dovoljeni časi prenosa določeni za posamezno alarmno sporočilo in ne za aritmetično sredino vseh prenosov. To pomeni, da je v vsakem posameznem razredu določen največji dovoljen čas prenosa, ki ga nobeno preneseno alarmno sporočilo ne sme preseči. Največji dovoljeni časi prenosa za posamezne razrede so prikazani v tabeli 3 in so večji od časov iz tabele 2.

RAZRED	M0 [s]	M1 [s]	M2 [s]	M3 [s]	M4 [s]
Največji dovoljeni čas prenosa	Ni zahtev	480	120	60	20

Tabela 3: Klasifikacija alarmnih prenosnih sistemov po največjem dovoljenem času prenosa [2].

V primeru, ko je čas prenosa za alarmno sporočilo večji od dovoljenega za posamezni razred, bi se moral tak prenos dodatno označiti kot napaka sistema za prenos alarmov z ustreznim sporočilom o napaki.

V primeru izpada notranje povezave med alarmnim sistemom varovanega objekta in sistemom za prenos alarmov, bi moral alarmni prenosni sistem generirati alarmno sporočilo ali pa sporočilo o napaki, ki se mora prenesti do centra za sprejem alarmov.

KLASIFIKACIJA PO ČASU SPOROČILA O NAPAKI

Za sisteme z avtomatskim nadzorom je posebno pomembno opravljanje funkcije nadzora nad sistemom za prenos alarmov. Ob nastanku napake na sistemu za prenos alarmov je pomemben prenos sporočila o napaki (T-reporting time) do centra za sprejem alarmov, ki naj bo čim krajši.

RAZRED	T1	T2	T3	T4	T5	T6
Največji dovoljeni čas prenosa	32 dni	25 ur	300 minut	180 sekund	90 sekund	20 sekund

Tabela 4: Klasifikacija alarmnih prenosnih sistemov po času sporočila o napaki [2].

Čas za prenos sporočila o napaki je definiran kot čas od nastanka napake na sistemu za prenos alarmov do trenutka, ko se ustrezno sporočilo o napaki pojavi v centru za sprejem alarmov ali v varnostnem nadzornem centru. Ta čas obsega tudi generiranje ustreznega sporočila o napaki in

njegov prenos po prenosnih poteh sistema za prenos alarmov. Čas ne bi smel presegati vrednosti za posamezne razrede podane v tabeli 4.

V sistemih s povečanim številom prenosnih poti in dodatno opremo bi morale biti zaradi zagotovitve zadostne propustnosti alarmnih sporočil v izrednih situacijah nadzirane vse dodatne prenosne poti in oprema. Vse dodatne prenosne poti in oprema bi morale imeti ob javljanju napake zagotovljene vrednosti časov prenosov sporočil znotraj ustreznih razredov iz tabele 4.

KLASIFIKACIJA PO RAZPOLOŽLJIVOSTI ALARMNEGA PRENOSNEGA SISTEMA

Razpoložljivost sistema (A-availability of the network) za prenos alarma je čas, izražen v odstotkih, v katerem je sistem za prenos alarmov sposoben prenesti sporočilo o alarmu s kateregakoli nanj priključenega alarmnega sistema do alarmnega sprejemnega centra. Pri prenosu, ki mora biti znotraj okvirov zahtevanih časov prenosa, se podatki ne smejo izgubiti. Sistemi za prenos alarmov se glede razpoložljivosti delijo v štiri razrede, ki jih prikazuje tabela 5.

RAZRED	A0	A1	A2	A3	A4
Razpoložljivost v kateremkoli 12 mesečnem obdobju	Ni zahtev	97%	99,3%	99,5%	99,8%
Mesečna razpoložljivost	Ni zahtev	75%	91%	95%	98,5%

Tabela 5: Klasifikacija alarmnih prenosnih sistemov po razpoložljivosti [2].

5. Opis naprav za protivlomno varovanje objektov

Pri izbiri protivlomnega alarmnega sistema moramo največ pozornosti nameniti alarmni centrali. Alarmna centrala je del alarmnega sistema, ki mora zadoščati potrebam in željam uporabnika. Pri nakupu alarmne centrale je treba premisliti o:

- številu senzorjev v sistemu (število senzorjev v sistemu vpliva na število področij, ki jih ima alarmna centrala). Področje je definirano kot katerikoli javljalnik (senzor, magnetni kontakt), ki pokriva določeno področje (cono),
- številu particij (sistem lahko razdelimo na več samostojnih podsistemov, npr. zaščita stanovanjskega dela in poslovnega dela, če imamo doma samostojno podjetje). Particija je definirana kot popolnoma ločen podsistem, ki deluje neodvisno od drugega. Tako imamo lahko več različnih particij na eni sami alarmni centrali,
- številu tipkovnic (možnost vklopa alarma z več mest),
- način komunikacije ob alarmu (vgrajen gsm-komunikator, možnost klica nadzornega centra, možnost klica na privatno telefonsko številko (običajno lastnik stanovanjskega objekta), prenos sporočil po telefonskem omrežju, internetu ali omrežju GSM),
- razširljivost sistema (ali imamo v prihodnosti namen razširiti objekt, možnost povečanja področij s pomočjo razširitvenih modulov, povečanja števila particij).

5.1. Alarmna centrala

Alarmna centrala predstavlja glavno kontrolno enoto protivlomnega alarmnega sistema. Vse naprave in senzorji so priključeni na njo. Njena funkcija je obdelava signalov, ki jih sprejema od senzorjev, tipkovnic in različnih modulov (govornih modulov, relejnih modulov), krmiljenje siren in prenos alarmnega signala. Alarmna centrala nudi tudi povezavo z video nadzornimi sistemi in sistemi vstopne kontrole. Alarmna centrala za svoje delovanje vedno potrebuje omrežno napajanje, transformator za prilagoditev napetosti in akumulator. Vsak alarmni sistem je neodvisen od omrežnega napajanja. V primeru izpada električne napetosti, centrala in s tem celoten sistem deluje normalno, saj se sistem preklopi na akumulatorsko napajanje [7].

Običajno je elektronika alarmne centrale skrita v kovinski omarici, kjer je mesto tudi za transformator in akumulator. V primeru novogradnje je možno kovinsko omarico vgraditi tudi podometno in s tem še mehansko povečati stopnjo zaščite.

Danes imajo praktično vse alarmne centrale vgrajen komunikator, ki omogoča vezavo na telefonsko linijo. Kam bo alarmna centrala klicala v primeru alarma je odvisno od nastavitve sistema. Centrala lahko pokliče nadzorni center in s pomočjo tonskega formata v samo nekaj sekundah prenese številko objekta, s katerega prihaja alarm ter področje vloma. Alarmno centralo lahko sprogramiramo tudi tako, da pokliče privatno telefonsko številko (mobilni telefon ali stacionarno številko) [7].

Včasih je težko razpoznati vse možnosti, ki jih alarmna centrala nudi. Točno sliko delovanja lahko ustvarimo šele po pregledu tehničnih specifikacij in navodil za uporabo.

5.2. Tipkovnica (šifrator)

Tipkovnica je namenjena komuniciranju uporabnika z alarmno centralo. Preko nje najpogosteje vnašamo gesla za vklop in izklop sistema in za pregled stanja sistema. Monter ali serviser preko nje nastavi delovanje celotnega alarmnega sistema. Celotno upravljanje alarmnega sistema je možno preko ene ali več tipkovnic. Za razliko od alarmne centrale, do katere ni potreben pogost dostop, je tipkovnica vedno na očeh uporabnika, saj se z njo vsakodnevno srečujemo. Tipkovnice se vgrajujejo v notranjosti pri vhodnih vratih in v zgornji etaži, če ima zgradba več etaž. To naredimo zato, da je možen vklop nočnega režima. Ko nastavimo delovanje nočnega režima se proženje alarma izklopi tistim senzorjem, ki so definirani kot nočno varovanje. V normalnem režimu je proženje alarma vklopljeno za vse senzorje.

Zelo pomembno je tudi, da je tipkovnica pregledna in enostavna za uporabo ter da ima možnost uporabe funkcijskih tipk. Z uporabo funkcijskih tipk lahko z enim pritiskom vklopimo ali izklopimo sistem v nočnem ali normalnem režimu. Funkcijskim tipkam lahko nastavimo tudi druge lastnosti.

5.3. Senzorji

Senzorji se delijo na aktivne in pasivne. Aktivni potrebujejo za svoje delovanje vir energije, izhodni alarmni signal pa nastane kot posledica spremembe te energije. Pasivni pa za svoje delovanje ne rabijo nobenega posebnega energijskega vira. Za njihovo delovanje zadostuje sprememba določene fizikalne veličine, ki jo povzroči oseba v območju detekcije senzorja. V to skupino spada tudi pasivni infrardeči javljalnik, ki izkorišča piroelektrične lastnosti določenih kristalov.

Pri primerjavi lastnosti obeh tipov senzorjev imajo aktivni boljše detektorske karakteristike, povzročajo manj lažnih alarmov in imajo boljše razmerje signal šum. Slaba stran aktivnih senzorjev je njihova višja cena, večja možnost odkritja ter medsebojni vpliv drug na drugega v primeru večjega števila aktivnih senzorjev. Prednosti pasivnih senzorjev se kažejo v nizki ceni izdelave, enostavni montaži in veliki občutljivosti. Slaba stran teh senzorjev je njihova občutljivost na vpliv okolice, ker imajo alarmni prag zelo malo nad motnjami okolice in s tem majhno razmerje signal šum. Posledica tega je veliko število lažnih alarmov.

Poleg tega delimo senzorje še na senzorje za notranjo in zunanjo uporabo. Pri notranjem varovanju se največkrat uporabljajo senzorji, ki pri odkrivanju vlomilcev uporabljajo bodisi zvočno valovanje visokih frekvenc (ultrazvočni senzorji) bodisi elektromagnetno valovanje visokih frekvenc (mikrovalovni senzorji) ali pa zaznavajo infrardeče sevanje vsiljivca (pasivni infrardeči senzorji). Vse bolj se uporabljajo tudi kombinirani senzorji, ki združujejo posamezne principe delovanja.

Naprave za zunanje varovanje varujejo zunanje površine pred vlomilci. Zunanji senzorji so prva prepreka vlomilcu. Ker so te naprave nameščene zunaj, morajo imeti večjo odpornost na temperaturne spremembe, vremenske pogoje in mehanske obremenitve.

Senzor protivlomnega alarmnega sistema zaznava spremembe na območju katerega varuje. Vsak senzor je vezan na centralo ali razširitveni modul. Centrala čaka na prejeti signal senzorja in ga ustrezno obdela. Odvisno od nastavljenega področja, alarmna centrala sproži nastavljeno akcijo in po potrebi sproži alarm. Za protivlomno varovanje imamo na voljo več različnih vrst senzorjev, ki se razlikujejo glede na uporabljeno tehnologijo zaznavanja sprememb:

- Notranji pasivni infrardeči senzor premika (PIR),
- Notranji senzor premika dvojne tehnologije (PIR & MW),
- Zunanji infrardeči in kombinirani senzor premika,
- Senzorji loma stekla,
- Magnetni kontakti,
- Bariere,
- Požarni senzorji.

Pri kvaliteti senzorjev moramo biti zelo pozorni. Glede na zahtevano stopnjo varnosti nam kvaliteto senzorjev določajo naslednji kriteriji:

- Zanesljivost detekcije,
- Sabotažna zaščita,
- Odpornost na lažne alarme.

Kriterija zanesljivost detekcije in odpornost na lažne alarme si med seboj nasprotujeta. Zanesljivost detekcije je boljša, če je občutljivost senzorja večja. Ko pa je občutljivost senzorja večja, je tudi večja možnost lažnih alarmov.

5.3.1. Notranji pasivni infrardeči senzor premika (PIR)

Uporaba PIR senzorjev je najbolj razširjen način varovanja prostorov. Senzor zaznava spremembe infrardeče energije v polju, ki ga senzor pokriva. Senzor v bistvu izkorišča dejstvo, da vsako telo, ogreto nad temperaturo absolutne ničle (0 K), seva v prostor infrardečo energijo. Tudi človek seva infrardečo energijo. Najmočnejše sevanje imamo pri glavi in rokah, katerih nimamo pokritih z oblačili.

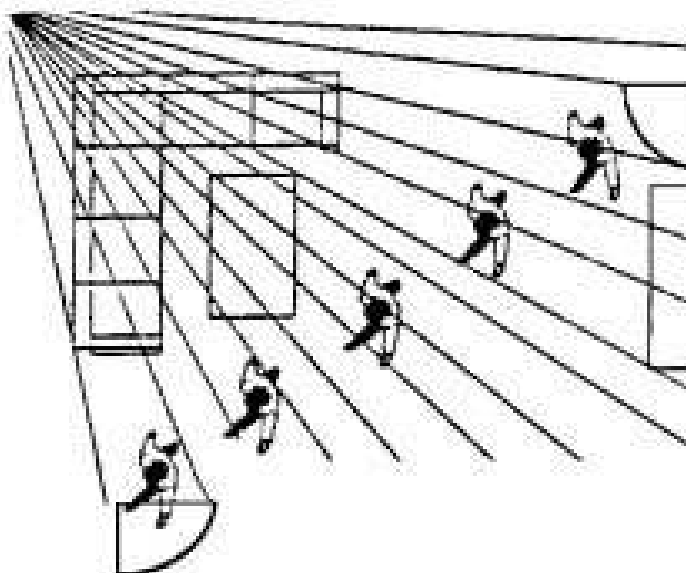
Ko senzor zazna spremembo, generira električni signal ter ga pošlje centrali. Pri senzorjih je potrebno posebno pozornost posvetiti uporabljenemu infrardečemu elementu, odpornosti senzorja na zunanje motnje (mobiteli, oddajniki,...) in temperaturni kompenzaciji (sposobnost senzorja, da se prilagodi višanju temperature v prostoru in vseeno ohrani zaznavanje). PIR senzorji imajo tudi možnost prilagajanja polja pokritja z menjavo leč in sabotažno zaščito senzorja s stikalom, ki preprečuje nepooblaščen odpiranje senzorja. Infrardeči senzorji se razlikujejo glede na način vgradnje in polje zaznavanja. Polja pokritja senzorjev se razlikujejo glede na uporabljeno lečo in vrsto IR elementa.

ZGRADBA IN DELOVANJE PASIVNEGA INFRARDEČEGA SENZORJA

PIR senzor je sestavljen iz pirodetektorja, električnega vezja in optike. Naloga pirodetektorja je zaznavanje sprememb infrardečega sevanja določene valovne dolžine. Odziv na spremembe infrardečega senzorja se kaže v velikosti izhodne napetosti. Najpomembnejša pokazatelja kvalitete pirodetektorja sta napetostni odziv pri danem infrardečem sevanju in velikosti šuma, ki nastane v njem.

Električno vezje je glavna logika senzorja, ki odloča kdaj se bo senzor sprožil. Najpomembnejši del električnega vezja je pasovni filter, ki ojačuje frekvenčni spekter alarmnega signala in duši motnje (šum). Najtežja naloga električnega vezja je torej odpornost proti lažnim alarmom, s tem se pa tudi kaže kvaliteta protivlomnega alarmnega sistema. Poleg javljanja alarma je naloga električnega vezja tudi zaščita proti sabotazi. Narejena je s sabotajnim stikalom. Stikalo je sklenjeno, ko je senzor pokrit s pokrovom. Alarmno stanje nastopi v primeru odstranjevanja pokrova.

Signal infrardečega sevanja od človeka, ki ga zazna pirodetektor, je občutno premajhen. Zato si pomagamo z optičnim sistemom za zbiranje IR sevanja. Optika zbira sevanje v področju, ki ga varuje senzor. Zbrane žarke nato strni in jih usmeri v pirodetektor. Zbiralna optika nam signal IR sevanj ojača za nekaj desetkrat, kar se bistveno pozna pri kvaliteti pirodetektorja. Velikost signala pirodetektorja je odvisna od velikosti spremembe infrardečega sevanja v času. Torej bo senzor zaznal vlomilca le, če bo ta povzročil dovolj veliko spremembo IR sevanja. Druga naloga optičnega sistema je, da razdeli varovano področje na občutljiva (aktivna) in manj občutljiva področja (pasivna). Pri prečkanju osebe mimo teh področij pride do znatne spremembe infrardečega sevanja in sproži se alarm. Primer osebe, ki prečka aktivna področja je prikazan na sliki 2.

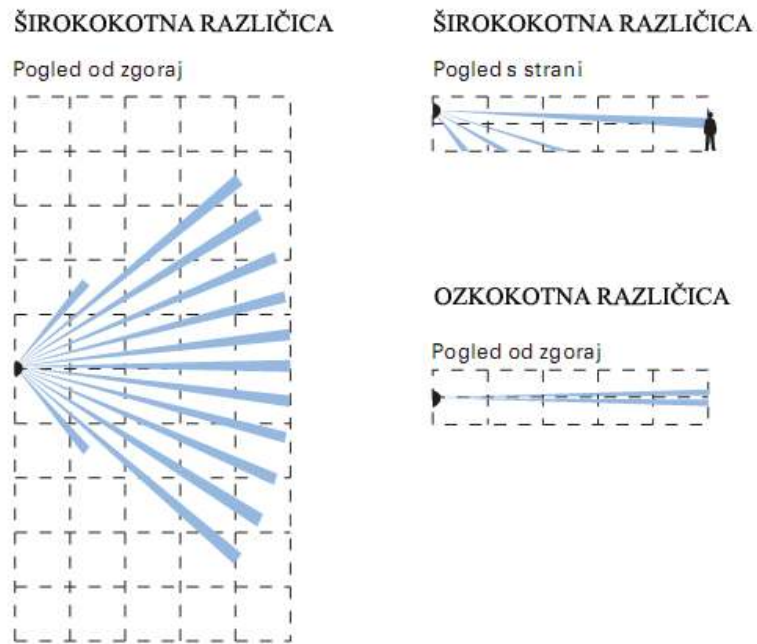


Slika 2: Primer prečkanja osebe mimo aktivnih in pasivnih področij senzorja [17].

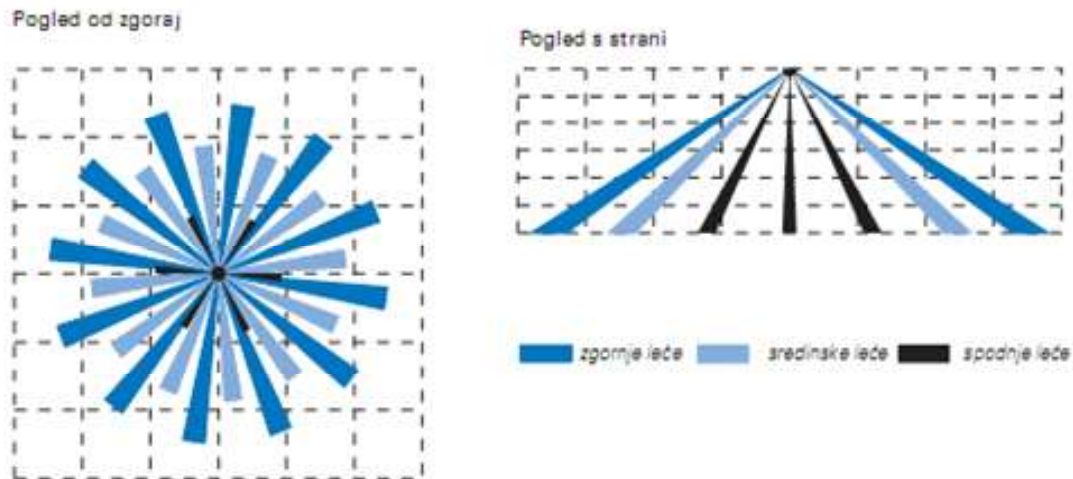
Oblika območja detekcije je pri senzorjih zelo različna. Diagram detekcije je določen s kombinacijo ogledal oziroma leč. Te se med seboj razlikujejo po kotu nadzora in številu

aktivnih področij. Glede na kot nadzora poznamo več vrst leč, kot so širokokotne, ozkokotne in 360° . Širokokotno različico uporabljamo v večini primerov. Če varujemo dolg in ozek hodnik bomo najverjetneje uporabljali ozkokotno različico. Primerjava diagramov pokritja širokokotne in ozkokotne različice je prikazana na sliki 3.

Senzor s 360° lečami vedno montiramo na strop ter s tem pokrijemo tudi dele, ki so za ostale senzorje nedosegljivi. Slika 4 nam prikazuje diagram pokritja senzorja pri 360° različici.



Slika 3: Primerjava diagramov pokritja senzorja pri širokokotni in ozkokotni različici.



Slika 4: Diagram pokritja senzorja pri 360° različici s tremi lečami.

PIR senzor je najbolj občutljiv na stranske pomike. To pa še ne pomeni, da senzor ne zaznava gibanja naprej in nazaj. Ker se aktivna področja širijo pahljačasto od senzorja, je praktično nemogoče narediti pomik parih metrov naprej in nazaj, ne da bi pri tem prečkali aktivno področje.

POSTAVITEV SENZORJEV IN ZMANJŠEVANJE ŠTEVILA LAŽNIH ALARMOV

Pri postavitvi alarmnega sistema je zelo pomembno, da nam ta ne javlja lažnih alarmov. Lažni alarm je alarm, ki ni nastal kot posledica vdora vlomilca in je kot takšen nezaželen. Vzroki za nastanek lažnega alarma so različni: okvara v napravi, vremenski vplivi, živali, človeške napake, potresi, itn. Možne vzroke za lažni alarm lahko preprečimo tudi sami, če upoštevamo naslednje vplive pri izbiri položaja senzorja [8]:

a) ELEKTROMAGNETNO SEVANJE

Senzor vedno vgradimo v stran od naprav, ki povzročajo elektromagnetno sevanje [9]. Ko tako napravo priključimo na omrežno napetost, v njeni okolici nastane električno polje. Jakost električnega polja (E) merimo v voltih na meter (V/m). Večja je napetost večje je električno polje. Za sproščanje električnega polja ni pomembno, da naprave deluje. Lahko je tudi izklopljena in je s tem v napravi napetost, čeprav tok skozi njo ne teče. Magnetno polje pa nastane le takrat kadar je naprava vključena in teče skozi njo električni tok. Tako je v stanovanju, kjer imamo priključene električne naprave, tako električno in magnetno polje. Čim večja je poraba električne energije in s tem električnega toka, tem večje je magnetno polje. Jakost magnetnega polja (H) merimo v amperih na meter (A/m). V praksi se pogosto uporablja gostota magnetnega pretoka (B) v teslih ($1T = 1 \text{ Vsm}^{-2}$).

Električno in magnetno polje se z oddaljenostjo od vira sevanja zelo hitro zmanjšujeta. Najmočnejša nizkofrekvenčna električna polja so pod visokonapetostnimi daljnovidni, najmočnejša magnetna polja nizkih frekvenc pa so v neposredni bližini električnih motorjev in drugih električnih naprav v gospodinjstvu.

Električna naprava	E (V/m)
Sušilnik za lase	0,060
Stereo sprejemnik	0,180
Likalnik	0,120
Hladilnik	0,120
Mešalnik	0,100
Opekač	0.080
TV	0,060
Aparat za pripravo kave	0,060
Sesalnik	0,050
Električna pečica	0,008
Žarnica	0,005

Tabela 6: Jakost električnega polja (E) v oddaljenosti 30 cm od naprav [9].

Električna in magnetna poljska jakost nista odvisni od velikosti, zapletenosti, moči in glasnosti električne naprave. Nekateri sušilniki za lase povzročajo zelo močna polja, drugi pa skoraj nič. Razlike v magnetni poljski jakosti so odvisne od tega, kako je naprava zasnovana. V tabeli 6 so podane jakosti električnih polj v oddaljenosti 30 cm za različne naprave v gospodinjstvu. Vrednosti gostote magnetnega pretoka pri električnih napravah na različni oddaljenost so podane v tabeli 7.

Električna naprava	B(μ T) pri oddaljenosti od naprave:		
	3 cm	30 cm	1 m
Sušilnik za lase	6 – 200	0,01 – 7	0,01 – 0,03
Brivnik	15 – 1500	0,08 – 9	0,01 – 0,03
Sesalnik	200 – 800	2 – 20	0,13 – 2
Radijski sprejemnik	16 – 56	1	<0,01
Električna peč	1 – 50	0,15 – 0,5	0,01 – 0,04
Pralni stroj	0,8 – 50	0,15 – 3	0,01 – 0,15
Likalnik	8 – 30	0,12 – 0,3	0,01 – 0,03
Pomivalni stroj	3,5 – 20	0,6 – 3	0,07 – 0,3
Kopirni stroj	1 – 5	0,2 – 0,8	<0,01
Faks	8 – 20	1 – 2	0,02 – 0,25
Osebni računalnik	0,5 – 30	0,1	<0,01
Hladilnik	0,5 – 1,7	0,01 – 0,25	<0,01
TV-sprejemnik	2,5 – 50	0,04 – 2	0,01 – 0,15
Fluoresc. Svetilka	40 – 400	0,5 – 2	0,02 – 0,25

Tabela 7: Vrednosti magnetnega polja (B) od različnih oddaljenosti od naprav [9].

b) VGRADNJA V MAJHNIH PROSTORIH

V majhnih prostorih je senzor bolj občutljiv na temperaturne spremembe kot v normalnih in velikih prostorih. Zaradi majhnega prostora so vse stvari bližje senzorju, zato senzor ne usmerjamo proti oknom, vratom, klimatski napravi, itn. V primeru varovanja takega prostora moramo PIR senzorju zmanjšati občutljivost zaznavanja temperaturnih sprememb. Če tudi to ne prepreči lažnih alarmov, prostor zavarujemo z magnetnimi kontakti ali s kombiniranimi senzorji.

c) SONČNA SVETLOBA

Izvor sončne svetlobe predstavlja za senzor dodatno polje in lahko spremeni temperaturo na površini leče senzorja. To lahko privede do lažnega alarma, zato senzor ne usmerjamo proti oknom in drugim steklenim površinam.

d) NAPRAVE, KI LAHKO SPREMENIJO TEMPERATURO

Klimatske naprave, razni grelci in radiatorji spreminjajo temperaturo, zato senzorjev ne usmerjamo vanje.

e) PREMIKAJOČI OBJEKTI

Senzorje ne usmerjamo v rastline, zavese in sušče perilo, ker lahko prav tako pride do lažnega alarma. Kjer se premikajo domače živali je najbolje, da imajo svoj prostor v katerem ni infrardečega senzorja premika. Te prostore raje zavarujemo z drugimi senzorji (magnetni kontakt) ali s senzorjem, ki ima nižji prag občutljivosti.

f) PREKRIVANJE POLJA POKRITJA SENZORJA

Senzor mora imeti čim večje polje pokritja. V primeru, da polje pokritja pokriva kakšna omara ali druga stvar, senzor ne bo deloval po pričakovanjih. Vlomilec lahko izkorišča postavljene predmete in s tem ne sproži alarma.

g) VGRADNJA V KOPALNICE IN VLAŽNEJŠE PROSTORE

Infrardeči senzor premika raje na vgrajujemo v kopalnice, saj je zaradi vlage in temperaturnih razlik njegova življenjska doba krajša, zanesljivost delovanja senzorja pa vprašljiva.

h) USMERJANJE SENZORJA

Nekateri postavljajo senzorje tako, da senzor pokriva možne vhode vlomilca. Vendar ta način ni najboljši, saj senzor zaznava spremembo najbolje, če se gibljemo pravokotno na smer polja pokritja. Tako senzor najhitreje zazna spremembo temperature znotraj polja pokritja in nam javi alarm. Izognemo se tudi temperaturnim spremembam, saj žarki ne pridejo neposredno do okna in vrat. Na sliki 5 je predstavljeno pravilno postavljanje senzorja v kot med dvema oknom.



Slika 5: Pravilna postavitev notranjega infrardečega senzorja premika med dvema oknom [8].

5.3.2. Notranji senzor premika dvojne tehnologije

Velikokrat je pri zahtevnejših aplikacijah zahtevana večja zanesljivost ali učinkovitost delovanja protivlomnega alarmnega sistema. Učinkovitost delovanja je boljša, če je število lažnih alarmov čim manjše. V tem primeru se uporabljajo senzorji dvojne tehnologije. Tak senzor v sebi združuje infrardečo (IR) in mikrovalovno (MW) zaznavanje. Za proženje alarma v tem primeru potrebujemo signal z obeh senzorjev. Infrardeči senzor premika zaznava spremembo temperature, mikrovalovni pa vstop objekta v polje varovanja. Zaradi dvojnega delovanja odpadejo vsi vzroki za lažni alarm, ki smo jih opisali pri PIR senzorjih. Tak senzor vedno uporabljamo v prostorih s kaminom (dnevna soba), kurilnici in neogrevani garaži. V

teh prostorih se bo lahko sprožil PIR senzor, MW senzor pa ne bo zaznal premika. Ker so ti senzorji zelo zanesljivi, jih uporabimo za varovanje objektov, kjer je zahtevana visoka stopnja varnosti (banke, vojaški objekti, itn.).

Velika prednost senzorjev dvojne tehnologije je tudi možnost uporabe "antimasking" tehnologije. Ta nam omogoča zaznavanje sabotaže, kadar vlomilci s prekrivanjem ali lakiranjem sensorja skušajo preprečiti njegovo delovanje in s tem zaznavo gibanja v prostoru. Senzor v primeru prekrivanja leče sproži alarm, ne glede na to, ali ima uporabnik alarmni sistem vklopljen ali ne. Funkcija je primerna zlasti v javnih prostorih, nakupovalnih centrih in bankah, kjer je enostaven dostop do senzorjev.

Mikrovalovni senzorji delujejo na principu Dopplerjevega efekta, zato so zelo slabo občutljivi na stransko gibanje. Pri PIR senzorju pa je to ravno obratno, saj je zelo občutljiv na stranske (prečne) premike. Glavna slabost mikrovalovnega sensorja je valovanje izven prostora katerega varujejo. Še najbolj je problematično sevanje skozi okna in vrata. Vpliv zunanjih gibanj lahko zmanjšamo s primerno nastavitvijo občutljivosti sensorja. Ta slabost MW sensorja pa nam velikokrat pride tudi prav. V primeru varovanja skladišča, kjer se nahaja mnogo velikih predmetov, je prodiranje mikrovalovnega valovanja skozi trdne ovire zelo praktično. Vsi ti predmeti lahko potencialnemu vlomilcu služijo kot zaščita, če uporabljamo samo PIR senzorje.

Če povzamemo, je kombinirani senzor (PIR & MW) sestavljen iz treh delov:

1. Pasivni infrardeči senzor,
2. Mikrovalovni senzor,
3. Logika, ki povezuje oba elementa.

Kot smo že omenili, PIR senzor zaznava toplotno sevanje gibajočega se vlomilca. Mikrovalovni senzor pa deluje na principu Dopplerjevega efekta ter ugotavlja razliko med oddano in sprejeto frekvenco valovanja. Oba dela pa sta povezana z logično funkcijo IN ali ALI. Pri IN načinu senzor sproži alarm le, če v določenem časovnem intervalu reagirata oba elementa. S tem načinom zmanjšamo možnost lažnega alarma ter izboljšamo zanesljivost detekcije. Z ALI načinom pa se združijo tako prednosti, kot tudi slabosti enega ali drugega elementa. Prag detekcije se sicer izboljša, vendar se hkrati poveča število lažnih alarmov.

DOPPLERJEV POJAV

Pojav se imenuje po avstrijskem matematiku in fiziku Christianu Andreasu Dopplerju. Dopplerjev pojav je fizikalni pojav, kjer zaradi gibanja izvora, ponora ali obeh nastane navidezna razlika v frekvenci oziroma valovni dolžini zvoka ali svetlobe. Če se izvor (senzor) ali ponor (vsiljivec) približujeta, se dopplerjeva frekvenca poviša. V obratnem primeru, ko se izvor in ponor oddaljujeta, pa se dopplerjeva frekvenca zniža. Ko mikrovalovni senzor zazna spremembo frekvence, nam ta javi alarm.

DELOVANJE MIKROVALOVNEGA SENZORJA

Mikrovalovni senzor je sestavljen iz oddajnika z oddajno anteno in sprejemnika s sprejemno anteno. Danes se za protivlomni sistem uporabljajo predvsem senzori, ki imajo združen tako oddajni kot sprejemni del in samo eno oddajno-sprejemno anteno.

Oddajnik preko svoje antene stalno oddaja signal visoke frekvence. Ko ta signal doseže oviro, se odbije in vrne do antene sprejemnika. Ravno tako pride do sprejemne antene signal, ki se odbije od človeka ali druge premikajoče se ovire. V tem primeru se bo sprejemna frekvenca signala (odbite frekvenca) razlikovala od oddajne. Ker del odbitega signala dobimo direktno na sprejemnik, bo oddajna frekvenca različna od sprejemne frekvence, ki se odbije od vlomilca. Razlika teh dveh frekvenc je posledica Dopplerjevega efekta. Senzor bo tako zaznal spremembo in sprožil alarm.

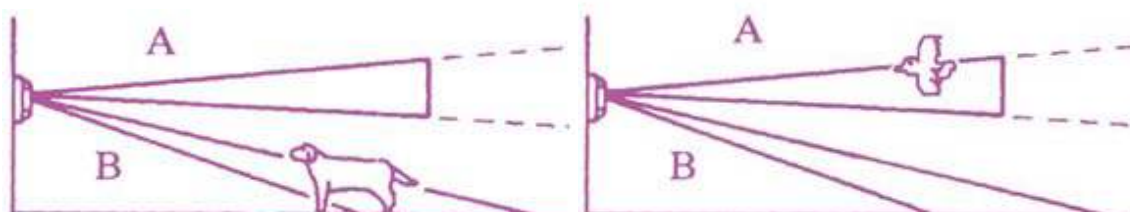
5.3.3. Zunanji senzor premika

Veliko objektov je danes varovanih samo od znotraj. Če hočemo preprečiti vlomilcu vstop v objekt, moramo postaviti tudi zunanje varovanje. S tem lahko učinkovito preprečimo tudi poškodbe, ki se pri vlamu zgodijo na vratih, oknih in drugih predmetih. To dosežemo s tem, da vlomilca zaznamo in prestrašimo z pravilno postavitvijo senzorjev. Tako je sistem izredno učinkovit, saj zazna vlomilca pred vstopom v objekt in omogoča učinkovito posredovanje.

Pogoji delovanja infrardečega senzorja na odprtem prostoru so povsem drugačni kot v primeru notranje vgradnje. Direktni vpliv sonca, vlage, živali in nizke temperature so dejavniki, ki jih ne smemo zanemariti. Kakovost izdelave je zato bistvenega pomena. Domet zunanjega senzorja je izredno težko omejiti, zato naj bo vedno usmerjen k objektu. Za učinkovito zaščito brez lažnih alarmov se priporoča uporaba funkcije proti živalim, kar pomeni, da senzor nima spodnjega področja zaznavanja. Velikokrat imajo senzori vgrajeno fotocelico, ki določa način delovanja v dnevnem ali nočnem režimu. Če torej hočemo uporabiti zanesljiv zunanji senzor, moramo upoštevati naslednje [8]:

a) TEHNOLOGIJA DELOVANJA IN VPLIV ŽIVALI

Zunanji senzor naj vedno uporablja funkcijo proti živalim. Senzor je sestavljen iz dveh IR elementov, ki polje zaznavanja prekrivata izmenično v pasovih.



Slika 6: Primer delovanja senzorja sestavljenega iz dveh IR elementov [8].

b) VPLIV SONCA

Vpliv sonca poveča verjetnost, da pride do lažnega alarma. Pri montaži zunanjega senzorja se torej moramo izogibati direktni izpostavljenosti sončnim žarkom. Senzor z dvojnimi IR elementom je sicer imun na vpliv sonca, če sonce posije samo v enega od elementov.

c) TESNJENJE

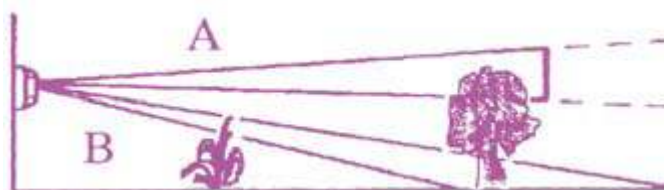
Zunanji senzorji so podvrženi različnim vplivom okolja. Poleg sonca je tukaj problem še pri dežju in snegu. Dobro tesnjenje je pomembno, da vlaga in voda ne prideta v elektroniko senzorja. Pri nakupu moramo biti pozorni pri standardu IP. Standard IP opisuje stopnjo zaščite in določa IP oznako, ki jo sestavljata dve številki. Prva številka opisuje zaščito pred dotikom s trdnimi predmeti, druga številka pa opisuje stopnjo zaščite pred vodo (tabela 8). Zadovoljivo zaščito nam zagotovi vsaj element z oznako IP54.

STANDARD IP		
	PRVA ŠTEVILKA(dotik)	DRUGA ŠTEVILKA(voda)
0	Brez zaščite	Brez zaščite.
1	Zaščita pred trdnimi delci velikosti večje od 50 mm (velika tuja telesa), oziroma zaščita pred naključnim dotikom roke.	Zaščita pred vertikalnim kapljanjem vode oziroma kondenzacijo.
2	Zaščita pred trdnimi delci velikosti večje od 12 mm (srednja tuja telesa), oziroma zaščita pred dotikom s prsti.	Zaščita pred direktnim škropljenjem z vodo, ko je naprava nagnjena za 15 stopinj (vertikalno) iz normalne lege.
3	Zaščita pred trdnimi delci večjim od 2,5 mm (majhna tuja telesa), oziroma zaščiti pred dotiki z orodji in žicami.	Zaščita pred direktnim škropljenjem z vodo, ko je naprava nagnjena za 60 stopinj (vertikalno) iz normalne lege.
4	Zaščita pred trdnimi delci večjim od 1 mm (zrnata tuja telesa), oziroma zaščita pred dotiki z finimi orodji in žicami.	Zaščita pred škropljenjem z vodo iz vseh smeri. Vstopna količina vode je omejena.
5	Zaščita pred omejeno količino prahu (brez škodljivih usedlin).	Zaščita pred vodnimi curki iz vseh smeri. Vstopna količina vode je omejena.
6	Popolna zaščita pred prahom, prah ne more prodreti v notranjost pri delnem tlaku 20 mbar-ov.	Zaščita pred močnimi vodnimi curki (uporaba na ladijski palubi). Vstopna količina vode je omejena.
7	/	Zaščita pred potopitvijo v vodo med 15cm in 100 cm (1 m) za krajši čas, pod določenimi časovnimi in tlačnimi pogoji.
8	/	Zaščita pred potopitvijo pod tlakom za daljši čas.

Tabela 8: Opis standarda zaščite IP [10].

d) TEMPERATURNE SPREMEMBE IN PREMIKANJE DREVES

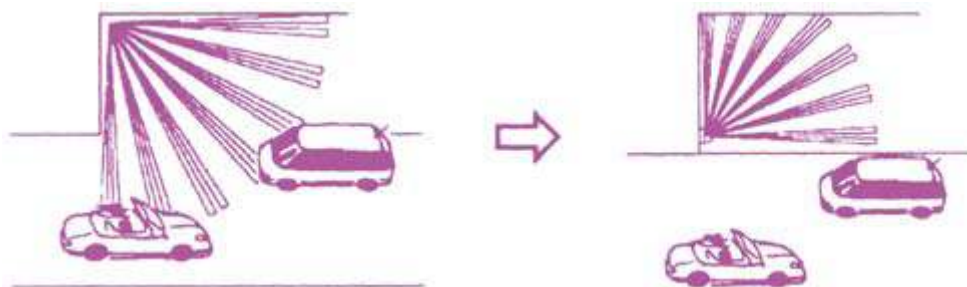
V polju pokritja ne sme prihajati do temperaturnih sprememb. Do temperaturnih sprememb pride ob nepričakovanem segrevanju predmetov ali sten, ki so v polju pokritja senzorja. Segrevanje kakšnih betonski sten lahko povzroči močnejše sonce v poletnem času. Pri postavitvi moramo paziti, da v polju pokritja ni dreves, grmovja in trave, ki lahko ob močnem vetru povzročajo neželene alarme.



Slika 7: Možni lažni alarm zaradi premikanja dreves [8].

e) VIŠINA MONTAŽE IN USMERJANJE ŽARKOV

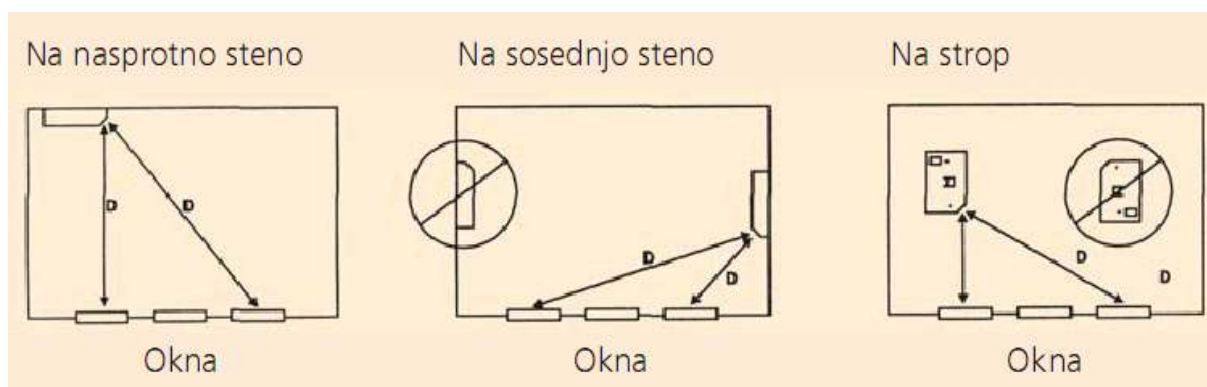
Pri višini montaže zunanjega senzorja moramo biti pozorni na višino montaže. Za pravilno delovanje mora biti senzor vgrajen na višini od 1 do 1,2 metra. Zaradi omejitve dometa infrardečih (IR) žarkov, naj bo senzor vedno usmerjen k objektu. Slika 8 (levo) nam prikazuje nepravilno postavitve senzorja, saj nam lahko alarm sprožijo prevozna sredstva ali sprehajalci ob cesti.



Slika 8: Nepravilno usmerjanje senzorja (levo) ter pravilna usmeritev senzorja v objekt (desno) [8].

5.3.4. Senzor loma stekla

V primeru, da so v objektu večje steklene površine, se priporoča uporaba senzorja loma stekla. Senzor povzroči alarm ob zaznavi specifične frekvence zvoka loma stekla, ravno tako pa je občutljiv tudi na rezanje steklenih površin. Senzor ni potrebno vgraditi na stekleno površino, ampak na steno ali strop (slika 9), le pozorni moramo biti, da je do možnega izvora loma stekla prosta pot. Prednost omenjenega senzorja je ta, da je lahko aktiven tudi v nočnem režimu delovanja, alarmni signal pa je sprožen še pred vstopom v varovani objekt. Tipično maksimalno pokritje senzorjev loma stekla je prostor do velikosti 10 x 10 m, senzor pa naj bo vedno usmerjen oknu. Učinkovita je kombinacija senzorjev loma stekla skupaj z magnetnimi kontakti v nočnem režimu, saj imamo takrat senzorje premika izklopljene. Možna postavitve senzorjev loma stekla je prikazana na sliki 9.



Slika 9: Možna postavitve senzorjev loma stekla [8].

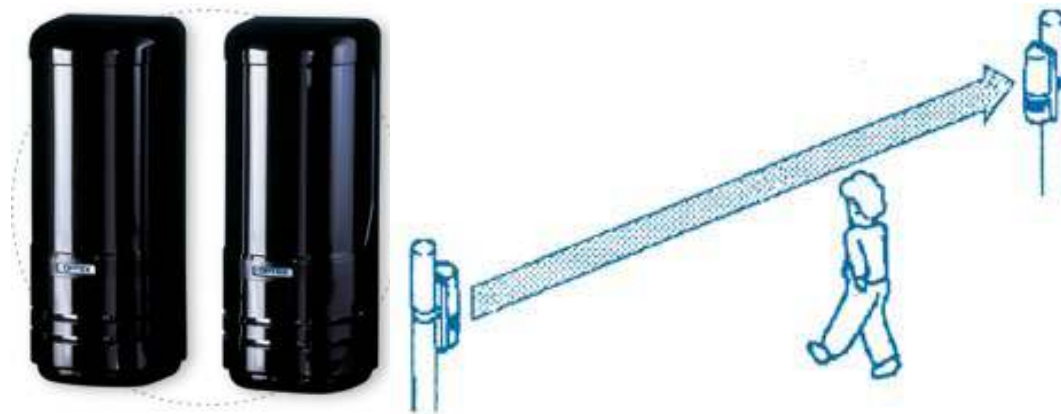
5.3.5. Magnetni kontakti

Pred uporabo infrardečih senzorjev premika, ki lahko zaznajo premik, so se za zaščito vrat in oken uporabljali magnetni kontakti. Vsa sodobna okna imajo že vgrajene magnetne kontakte in dve žici, ki ponazarjata stikalo magnetnega kontakta. Magnetni kontakti uporabljajo za

zaznavo magnetno polje, ki je v primeru odpiranja prekinjeno, kar sproži alarm. Prednost magnetnih kontaktov je nizka cena. V primeru nočnega režima s PIR senzorji ne pokrivamo vstopne dele v objekt, zato so magnetni kontakti v oknih in vratih dobra rešitev. Slabost tega varovanja pa je veliko število kablov za učinkovito zaščito.

5.3.6. Bariere (žarkovne zapore)

Za postavitev dodatnih ovir vlomilcu se velikokrat uporabljajo bariere. Vsaka bariera je sestavljena iz sprejemnika in oddajnika, med katerima poteka neviden IR žarek (slika 10). Prekinitev IR žarka sproži alarm. Bariere lahko uporabljamo za notranje (skladišča, hodniki) ali zunanje (parkirišča, dvorišča) aplikacije. Njihova uporaba bistveno pripomore k zanesljivosti alarmnega sistema. Priporoča se vgradnjo na steber, saj s tem povečamo polje pokritja. Pri postavitvi moramo biti pozorni na: vpliv sonca, zakrivanje polja pokritja (drevesa, grmovja), zunanje vplive (voda), višino montaže in nestabilno podlago.

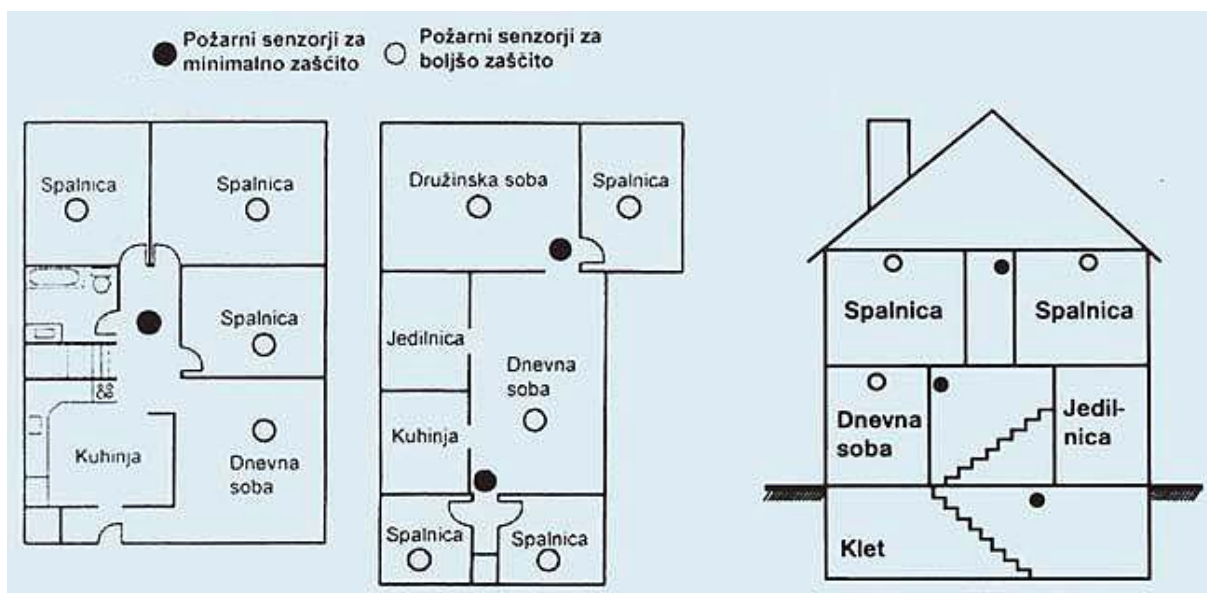


Slika 10: Primer sprejemnika in oddajnika bariere.

5.3.7. Požarni senzorji

Večina alarmnih central omogoča tudi vklop požarnih senzorjev. Področje centrale, kjer so priključeni požarni senzorji, je aktivno ne glede ali je sistem vključen ali izključen. Protivlomni senzorji so namreč aktivni samo ob vklopu alarmnega sistema. Za učinkovito zaščito objekta se priporoča vgradnjo vsaj enega požarnega senzorja v vsako etažo stanovanja. Smiselno jih je postaviti v prostore, kjer je večja nevarnost požara, kot so klet, prostor, kjer je postavljen kamin, kuhinja. Za priklop požarnega senzorja se v tem primeru uporablja enak priključni kabel kot za protivlomni senzor. Pri izbiri pozicije požarnih senzorjev moramo upoštevati sledeča pravila [3]:

- Vedno moramo zaščititi prehode med prostori, preko katerih prehajamo iz ene spalnice v drugo (slika 11, levo).
- Če je v objektu več ločenih spalnic, namestimo požarni senzor pri vsakem vhodu v spalnico (slika 11, sredina).
- V vsako nadstropje se priporoča vsaj eden dimni senzor.
- Sistem lahko zaščitimo minimalno ali postavimo boljše zaščito.



Slika 11: Izbira pozicij požarnih senzorjev za minimalno in boljšo zaščito [3].

5.4. Sirena

Glavna funkcija sirene je opozarjanje, da se je na objektu sprožil alarm. Na sireno nikoli ne smemo gledati kot moteči del alarmnega sistema. Morebitni vlomilec se v objektu, kjer deluje močna zunanja sirena, nikoli ne bo zadrževal dlje časa. Tu vidimo dobro stran varovanja, saj bodo ob vklopu sirene bolj pozorni sosede in mimoidoči. Pri sirenah ločimo sirene za notranjo in zunanjo vgradnjo. Najboljša kombinacija varovanja je, da uporabimo obe. Notranje sirene so praviloma manjše in neopazne. Skoraj vse zunanje sirene imajo svoje napajanje z vgrajenim akumulatorjem, kar pomeni, da sirena deluje neodvisno od alarmnega sistema. Tudi v primeru sabotáže sirene in prekinitve povezave do alarmne centrale bo sirena delovala. Zunanja sirena mora biti vgrajena čim bolj nedostopno na vrhu objekta. S tem je sirena bolj zaščitena pred sabotážo, zvok sirene pa je močnejši, kot če bi bila sirena vgrajena nižje. Na sliki 12 je prikazan izgled zunanjih siren.



Slika 12: Izgled zunanjih siren.

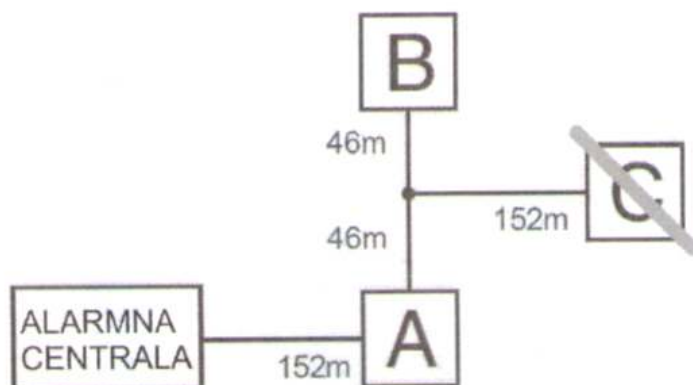
6. Primerjava alarmnih naprav proizvajalca DSC in njihovih lastnosti

Podjetje DSC (Digital Security Controls) je vodilni svetovni proizvajalec varnostnih sistemov, ki ima sedež v Kanadi. Priznan je v več kot 140 državah sveta. Podjetje razvija in proizvaja varnostne centrale, detektorje, senzorje, komunikacijske proizvode in strukturirano ožičenje. Njihov uspeh je viden zaradi nenehnega postavljanja novih standardov v zanesljivosti, fleksibilnosti, predstavitvi in vrednosti proizvodov, ki jih uporabljajo na vseh svetovnih kontinentih. Vse to je podjetju DSC omogočilo pridobiti vodilno vlogo v tehnologiji, proizvodnji in distribuciji varnostnih sistemov. Inovativni varnostni proizvodi se enostavno vgrajujejo, servisirajo in uporabljajo.

DSC teži k nenehnemu razvoju opreme tehničnega varovanja. Leto 2008 je prineslo tri nove alarmne centrale, ki predstavljajo povsem novo linijo proizvodov DSC. Nadgradnja central je bila potrebna, ker stara zasnova ni več omogočala prilagoditev novim izzivom in tehnologijam. Tako je nastala serija New Power, ki je vrhunec razvoja alarmnih central. Poleg central je tudi nova linija tipkovnic, ki jih odlikuje modern in nevsiljiv zunanji izgled [12].

6.1. Komunikacija KEYBUS med napravami

Za povezavo med centralo in ostalimi moduli se uporablja štirižilna povezava KEYBUS (dve žili za napajanje RDEČA- V_{DD} , ČRNA- V_{SS} in dve za prenos podatkov in urinega signala). Osnovni pogoj za medsebojno povezavo je, da dolžina povezave od alarmne centrale do kateregakoli modula, ne sme presegati 305 m. Celotna dolžina kabla ne sme presegati 915 m (slika 13).



Slika 13: Primer prevelike razdalje kabla med alarmno centralo in modulom C [12].

Komunikacija KEYBUS uporablja vodilo in protokol I^2C (I2C). I^2C vodilo je razvilo podjetje Philips Semiconductors v zgodnjih osemdesetih letih. Njegov osnovni namen je bilo enostavno povezovanje procesorja (CPU) s perifernimi enotami v TV-sprejemniku. Običajni računalniški sistemi uporabljajo paralelna vodila za opravljanje takšne naloge. Rezultat tega je

veliko bakrenih povezav na tiskanem vezju za podatkovne in naslovne linije. Tukaj je potrebna velika količina dekoderske logike, ki vse to povezuje. V izdelkih široke potrošnje, kot so audio-video naprave, je tako povezovanje nesprejemljivo. V teh napravah vsaka komponenta manj pomeni večji dobiček za proizvajalca in nižjo ceno za končnega potrošnika. Poleg tega ima veliko število linij za posledico, da je naprava bolj podvržena tako elektromagnetnim motnjam kot elektrostatičnim razelektritvam. Raziskava, ki so jo naredili v Philipsovih laboratorijih je imela za posledico novo dvožično vodilo imenovano I²C -vodilo ali I²C -bus. I²C je sinonim za Inter-IC bus. Že samo ime pove, da je namen vodila medsebojno povezati integrirana vezja [13].

I²C vodilo je serijsko vodilo, ki uporablja dve enosmerni liniji in asimetrični prenos. Ena linija služi za prenos serijskih podatkov (SDA – Serial Data), druga pa za prenos urinega signala (SCL – Serial Clock). Obe liniji sta s pull-up uporoma priključeni na pozitivno napajalno napetost, tako da sta v mirovnem stanju obe na logičnem nivoju 1. Po SDA liniji lahko podatki potujejo v obe smeri, vendar ne istočasno, kar imenujemo Half Duplex prenos. Vsaka naprava ima svoj unikatni 7 ali 10-bitni naslov. Vsaka od teh naprav je lahko oddajnik in sprejemnik, lahko pa je samo oddajnik ali pa sprejemnik, odvisno od njene funkcije. LCD prikazovalnik je logično samo sprejemnik. Na vodilu imamo torej lahko več naprav z vlogo gospodarja (ang. master) in več sužnjev (ang. slave) [13].

Na vodilu je neka naprava vedno gospodar (običajno mikrokrmilnik). Ta krmili signal SCL in začenja ter zaključuje prenose. Ostale naprave so v tem primeru sužnji. Kot smo rekli pa imamo na vodilu lahko tudi več gospodarjev. Če v tem primeru hoče naprava A poslati sporočilo napravi B si koraki komunikacije sledijo tako [13]:

- naprava A (gospodar) dodeli naslov napravi B (suženj),
 - naprava A (gospodar-oddajnik) pošlje podatke napravi B (suženj-sprejemnik),
 - naprava A prekine povezavo.
- Če pa hoče naprava A sprejeti informacijo od naprave B:
- naprava A (gospodar) dodeli naslov napravi B (suženj),
 - naprava A (gospodar-sprejemnik) sprejme podatke od naprave B (suženj-oddajnik),
 - naprava A prekine povezavo tudi v tem primeru, ko je naprava A sprejemnik.

Ko je vodilo prosto, sta liniji SCL in SDA na logičnem nivoju 1. Naprave, ki so priključene na vodilo I²C in niso aktivne imajo veliko impedanco. Obstajajo trije načini delovanja [13]:

1. Standard Mode – hitrost prenosa je do 100 kbit/s,
2. Fast Mode – hitrost prenosa je do 400 kbit/s,
3. High Speed Mode – hitrost prenosa je do 3,4 Mbit/s.

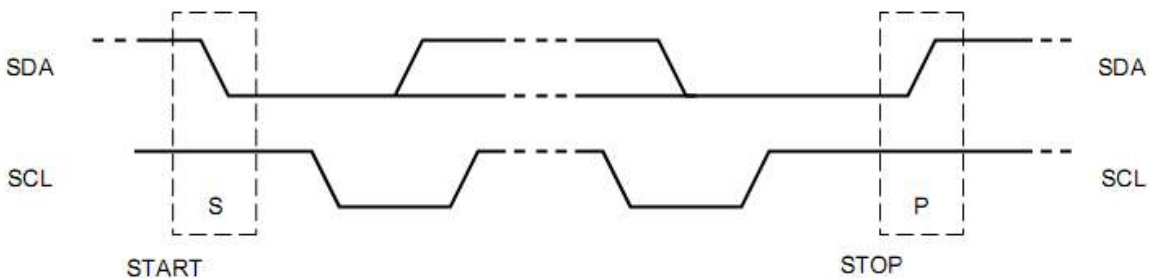
Število priključenih naprav na vodilu I²C je omejeno z velikostjo naslovnega prostora in kapacitivno obremenitvijo, ki je lahko največ 400 pF.

START in STOP stanji

V protokolu I²C sta definirani dve unikatni stanji, START (S) in STOP (P). Stanje START je definirano s prehodom iz visokega (HIGH – logični nivo 1) stanja v nizko (LOW – logični nivo 0) na liniji SDA, medtem ko je linija SCL v visokem stanju.

Stanje STOP pa je definirano s prehodom iz nizkega stanja v visoko pri liniji SDA, medtem ko je linija SCL v nizkem stanju.

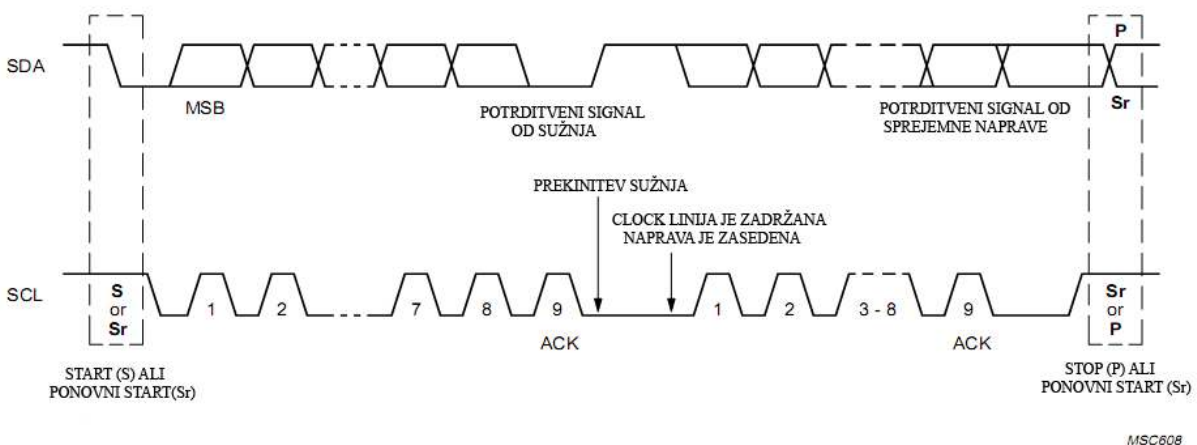
To sta edina primera, ko se signal SDA spreminja, medtem ko je urin signal SCL v visokem stanju. Med prenosom se signal SDA lahko spreminja samo, ko je SCL v nizkem stanju. Na sliki 14 imamo grafičen prikaz stanja START in STOP. Stanji START in STOP vedno generira gospodar. Linija je medtem zasedena, dokler nadrejena naprava ne generira stanje STOP. Linija ostane zasedena, če gospodar ponovno generira START bit (Sr) namesto STOP. V tem primeru sta START (S) in ponovni START (Sr) identična (slika 15).



Slika 14: Prikaz stanja START (S) in STOP (P) [13].

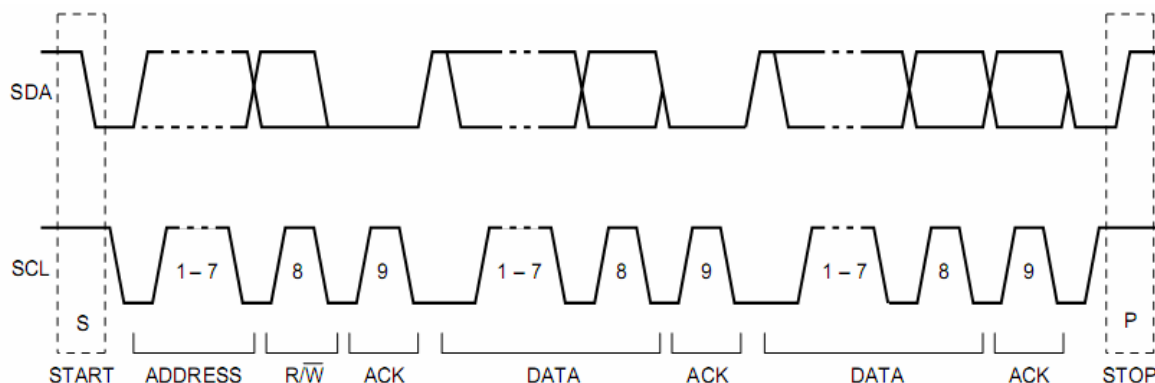
PRENOS PODATKOV

Podatki se vedno prenašajo v 8-bitnih enotah. Število poslanih bajtov gospodarja je neomejeno. Vsakemu bajtu sledi ACK bit. Če suženj ne more sprejeti ali oddati podatka (naprava zasedena), lahko zadrži SCL linijo v nizkem stanju in tako prisili gospodarja v čakanje (slika 15). Prenašanje podatkov se nadaljuje, ko je suženj pripravljen in ko suženj sprosti linijo SCL [13].



Slika 15: Podrejena naprava zadrži SCL linijo, ker je zasedena [13].

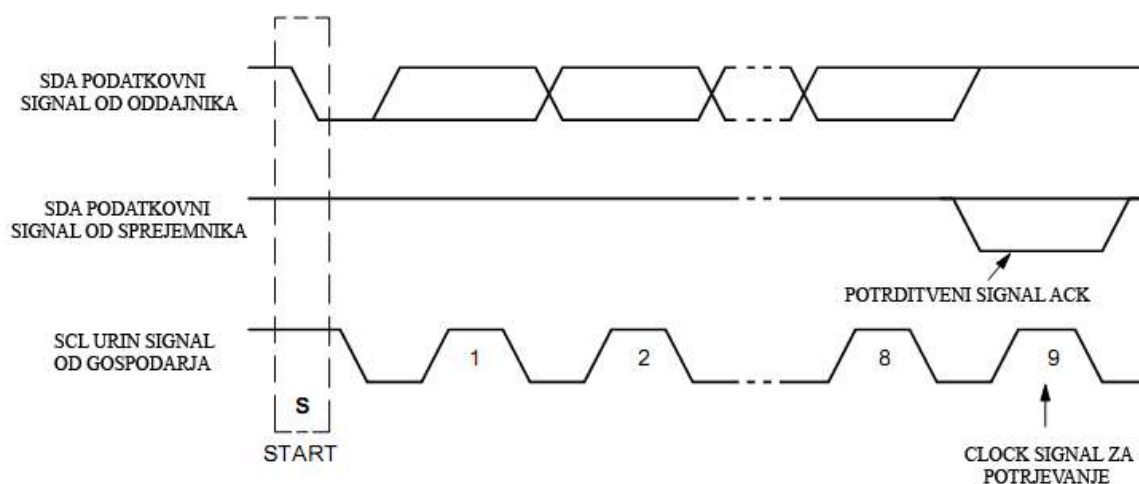
Zadrževanje linije SCL v nizkem stanju protokol uporablja tudi pri prehitrem sprejemanju in oddajanju podatkov. Tako lahko suženj zadrži linijo in obdela podatek. Ko je podatek shranjen ali pripravljen za prenos, suženj sprosti linijo.



Slika 16: Primer sprejemanja/pošiljanja dveh bajtov podatkov [13].

Slika 16 prikazuje časovni diagram podatkovnega signala SDA in potek urinega signala SCL. Ko naprave ne komunicirajo med seboj, sta oba signala v visokem stanju. Nato gospodar želi komunicirati s sužnjem, zato gospodar pošlje stanje START. Ko gospodar pošlje stanje START, vsi sužnji na vodilu čakajo na prihajajoče podatke. Nato gospodar pošlje 7-bitni naslov sužnja, s katerim želi komunicirati.

Vse naprave sprejmejo poslani naslov, če se naslov naprave ujema, suženj postane suženj-sprejemnik ali suženj-oddajnik, odvisno od osmega Read/Write bita. Če se naslov ne ujema, naprava ne naredi nič in čaka na stanje STOP. Z R/W bitom gospodar signalizira sužnju ali želi brati ali pisati. Če je R/W bit v nizkem stanju, želi gospodar brati podatke. V nasprotnem primeru, če ima omenjeni bit visoko stanje, pa želi gospodar pisati podatke.

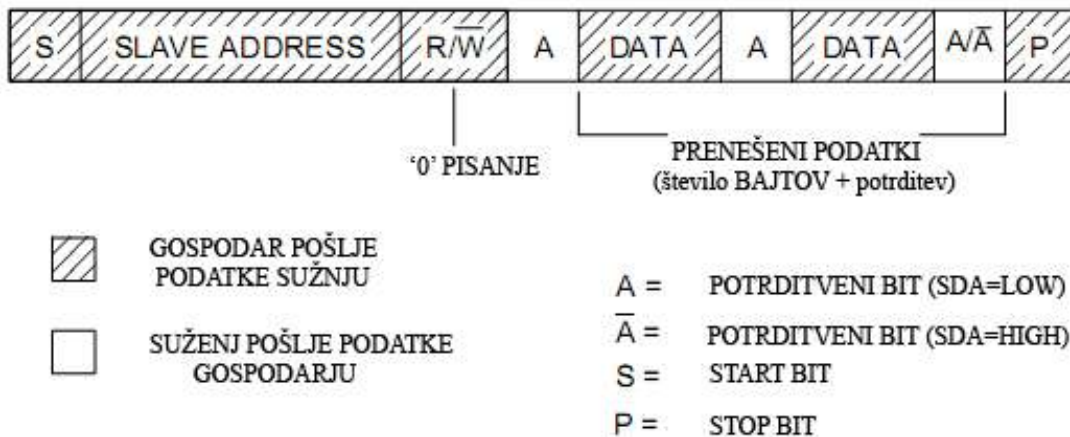


Slika 17: Primer potrditvenega signala ACK sprejemnika [13].

Pri vseh prenosih je obvezno potrjevanje na koncu vsakega prenesenega bajta. Zato sledi še deveti ali potrditveni bit (ang. ACK), ki ga generira gospodar. S tem gospodar sprosti SDA linijo. Sedaj mora SDA linijo v nizko stanje postaviti sprejemnik (gospodar ali suženj,

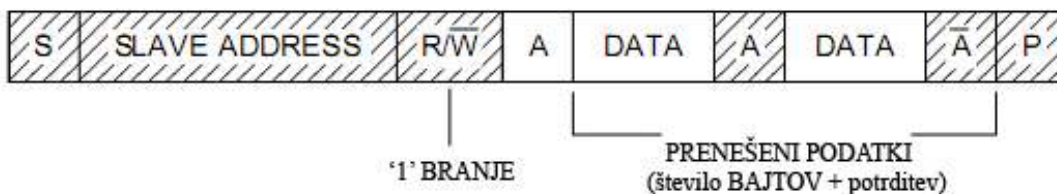
odvisno od smeri prenosa) tako, da SDA podatkovni signal ostane v nizkem stanju v času visokega nivoja SCL (slika 15, 16). Če sprejemnik SDA podatkovni signal ne postavi v nizek nivo, to pomeni, da podatka ni sprejel (slika 17) ali pa je naprava zasedena in je potrebno prenos ponoviti. Gospodar generira STOP ali ponovljeni START. Opisano velja za vse bajte znotraj prenosa, tako podatkovne kot naslovne in ukazne.

Nato, v primeru pisanja (slika 18), gospodar (oddajnik) po SDA liniji pošlje podatek sužnju (sprejemnik). S tem gospodar izbere register, ki bi ga rad v nadaljevanju bral. Zopet sledi potrditveni bit sprejemnika, s katerim je potrdil, da je podatek sprejel.



Slika 18: Primer pisanja nadrejene naprave v podrejeno [13].

V primeru branja suženj gospodarju pošlje podatek, ki ga hoče prebrati. Takoj po prvi potrditvi (slika 19) gospodar-pošiljatelj postane gospodar-sprejemnik in suženj-sprejemnik postane suženj-pošiljatelj. Zatem sledi še potrditveni bit sprejemnika (v tem primeru gospodar). Če sprejemnik ni potrdil sprejema podatka (SDA=HIGH), sporoča oddajniku, da želi končati komunikacijo. Če je v času potrditvenega bita SDA linija v nizkem stanju, je sprejemnik sprejel podatke.



Slika 19: Primer branja nadrejene naprave iz podrejene [13].

Sledi stanje STOP ali ponovni START (suženj ve, da je naslednji podatek del istega sporočila). Na ta način se sprosti vodilo, ki je pripravljeno na naslednji prenos podatkov.

6.2. Primerjava alarmnih central proizvajalca DSC

Podjetje DSC nudi veliko izbiro alarmnih central. Tabela 9 prikazuje primerjavo alarmnih central serije Power proizvajalca DSC.

	PC585	PC1565	PC5010	PC5020	EnvoyLCD	PC4020	PC6010
Število področij na plošči	4	6	8	8	32(brezžično)	16	16
Razširitev področij do	32	8	32	64	32	128	256
Širitev preko dodatnih tipkovic	DA	DA	DA	DA	NE	NE	NE
Žična širitev	NE	NE	DA	DA	do 2	DA	DA
Brezžična širitev	DA	DA	DA	DA	DA	DA	NE
Adresabilna širitev	NE	NE	DA	DA	NE	DA	NE
Število tipkovic	8	8	8	8	vgrajena	16	64
Število brezžičnih sprejemnikov	4	4	4	4	vgrajena	8	NE
Število nizko-tokovnih izhodov PGM (plošča)	2	1	1	3	do 2	1	1
Dodatna širitev nizko-tokovnih izhodov PGM	NE	8	8	8	NE	144	144
Število visoko-tokovnih izhodov PGM (plošča)	NE	1	1	1	NE	1	1
Dodatna širitev visoko-tokovnih izhodov PGM	NE	4	4	4	4	64	64
Število uporabniških gesel	38	38	38	38	38	1500	1000
Število particij	1	2	2	8	NE	8	32
Spomin dogodkov	128	128	128	256	128	3000	3000
Nadzor telefonske linije	DA	DA	DA	DA	DA	DA	DA
Nadzor sirene	DA	DA	DA	DA	DA	DA	DA
Funkcija SIA	DA	DA	DA	DA	DA	NE	NE
Prenos na pager	DA	DA	DA	DA	DA	DA	NE
Upload/download podpora	DA	DA	DA	DA	DA	DA	DA
Podpora direktnega downloada	DA	DA	DA	DA	DA	DA	DA
Podpora z DLS programsko opremo	NE	NE	NE	DA	NE	DA	NE
Alarmna komunikacija preko interneta	NE	NE	NE	DA	NE	DA	NE
Vizualna potrditev alarma	NE	NE	DA	DA	NE	NE	NE
Zvočna potrditev alarma	NE	NE	DA	DA	NE	NE	NE

Tabela 9: Primerjava alarmnih central serije Power pri proizvajalcu DSC [12].

Tabela 10 pa prikazuje primerjavo centrale PC585 serije Power in treh central serije New power pri DSC.

	PC585	PC1616	PC1832	PC1864
Področja na plošči	4	6	8	8
Možna širitev področij do:	32(brezžično)	16	32	64
Žične širitve	NE	16(1xPC5108)	32(3xPC5108)	64(7xPC5108)

Brezžična področja	32(4xRF5108)	16 (2xRF5108)	32 (4xRF5108)	32 (RF5108)
Širitev preko adresabilnih modulov	NE	DA	DA	DA
Število izhodov PGM	PGM1=50 mA PGM2=50 mA	PGM1=50 mA PGM2=300 mA	PGM1=50 mA PGM2=300 mA	PGM1,3,4=50 mA PGM2=300 mA
Širitev nizko-tokovnih izhodov	NE	8x50 mA (PC5208)	8x50 mA (PC5208)	8x50 mA (PC5208)
Širitev visoko-tokovnih izhodov	NE	4x500 mA (PC5204)	4x500 mA (PC5204)	4x500 mA (PC5204)
Število tipkovnic	8	8	8	8
Število particij	1	2	4	8
Število gesel	32 + glavno geslo	47 + glavno geslo	71 + glavno geslo	94 + glavno geslo
Spomin	128 dogodkov	500 dogodkov	500 dogodkov	500 dogodkov
Nadzor telefonske linije	DA	DA	DA	DA
Nadzor sirene	DA	DA	DA	DA
Klic na zasebno telefonsko številko	DA	DA	DA	DA
Izhod za sireno	DA	DA	DA	DA
Podpora uvoza in izvoza podatkov	DA	DA	DA	DA
PC-link z DLS programsko opemo	DA	DA	DA	DA
Mrežni prenos alarmnih signalov	NE	DA	DA	DA
Preverjanje alarma z video prenosom	NE	DA	DA	DA
Preverjanje alarma z zvočnim prenosom	NE	DA	DA	DA

Tabela 10: Primerjava alarmnih central serije New power pri proizvajalcu DSC [11].

Pri nakupu alarmne centrale gledamo predvsem na število področij na plošči in možno širitev žičnih in brezžičnih področij preko razširitvenih modulov. Razširitveni modul nam pomaga razširiti centralo na več področij. V stanovanju, kjer nimamo veliko javljalnikov, je nesmiselno kupiti alarmno centralo z veliko širitvenih področij. Pomembni so tudi podatki o številu tipkovnic, ki jih lahko priključimo na alarmno centralo, številu particij in številu uporabniških gesel.

Pri izbiri alarmne centrale je pomembno tudi število nizko-tokovnih in visoko-tokovnih programabilnih izhodov PGM na sami plošči in možnost njihove širitve. Tranzistorski izhodi ali izhodi PGM (Programabilni izhodi), nam omogočajo uporabo dodatnih izhodov ob sproženem dogodku. V centrali je izhod PGM definiran kot normalno odprto stikalo (NO), ki je povezano na maso (negativni pol). Ob določenem izpolnjenem dogodku, se stikalo sklene in ostane sklenjeno tako dolgo kot traja dogodek. Naprava, ki uporablja izhod PGM, mora biti priključena na pozitivni pol napajanja in izhod PGM. V trenutku, ko se izhod PGM aktivira na napravi, dobimo napetost.

Velikokrat nas zanima tudi način komunikacije v primeru sproženega alarma. Večina alarmnih central DSC podpira komunikacijska formata SIA in DTMF CONTACT ID, ki sta

potrebna za komunikacijo in sporazumevanje z varnostno nadzornim centrom v primeru alarma. Format CONTACT ID je nadgradnja komunikacijskega formata SIA, ki ga je razvilo podjetje ADEMCO Group. Primer dobljenega sporočila v formatu CONTACT ID, ki ga v nadzornem centru dekodirajo, bi bil:

1234 18 1130 01 015 8

Prve štiri številke (1234) so naročniška številka uporabnika. Drugi dve številki (18) sporočata sprejemniku, da je to sporočilo v formatu CONTACT ID. Naslednja številka (1) pomeni, da se je zgodil nov dogodek oziroma nov alarm. Namesto sedme številke je lahko tudi vrednost 3, ki pomeni, da se je dogodek spremenil v normalno stanje (restore). Če pa ima sedma številka vrednost 6, pa pomeni, da je prejšnji poslani dogodek še zmeraj aktiven. Sledijo tri številke, ki ponazarjajo kodo dogodka. Vrednost 130 pomeni, da je prišlo do vloma (Burglary). Naslednji dve številki pomenita številko particije. Vrednost 01 pomeni, da se je dogodek sprožil na prvi particiji. Naslednje tri številke določajo področje, na katerem se je sprožil dogodek. Vrednost 013 pomeni, da se je stanje spremenilo na področju 13. Na koncu sledi potrditvena številka (8).

Vse alarmne centrale proizvajalca DSC imajo na voljo nekaj specifičnih značilnosti [7]:

TLM (nadzor prisotnosti telefonske linije): Vse alarmne centrale DSC vedno spremljajo in kontrolirajo prisotnost telefonske linije. V primeru izpada telefonske linije lahko sistem sproži sireno ali uporabi kakšen drug način komunikacije – prenos signala preko omrežja GSM, proženja drugih oblik alarmiranja preko programabilnih izhodov PGM.

POMNILNIK DOGODKOV: Za učinkovito kontrolo delovanja imajo alarmne centrale tudi EEPROM pomnilnik za shranjevanje dogodkov. S tem uporabniku in VNC-ju poenostavimo varovanje, ko se sproži alarm. Kot vidimo v tabeli 10 običajne centrale omogočajo shranjevanje že do 500 dogodkov. To nam omogoča učinkovit nadzor dogajanja v preteklosti. Večje alarmne centrale pa imajo pomnilnik, ki omogoča shranjevanje vse do 3000 dogodkov.

PARTICIJE: Particija lahko deluje kot popolnoma ločen podsistem. Particija ima lahko svoja ločena gesla, področja in avtomatske vklope. V praksi to pomeni, da imamo v eni alarmni centrali več samostojnih sistemov. Najzmogljivejša alarmna centrala proizvajalca DSC ponuja 32 popolnoma ločenih sistemov.

FUNKCIJSKE TIPKE: Nekaterne funkcije alarmnega sistema, kot so vklop sistema ali vklop sistema v nočnem režimu bomo vsakodnevno uporabljali. Alarmne centrale DSC omogočajo uporabo funkcijskih tipk, ki z enim pritiskom izvršijo programirano funkcijo. Vsako funkcijsko tipko lahko tudi nastavimo na drugačno funkcijo, odvisno katero najbolj uporabljamo.

NASTAVITEV ZVOKA TIPKOVNICE: Akustična indikacija vstopa in izstopa je nastavljiva tako z jakostjo kot vrsto zvoka. Zvok lahko tudi izklopimo.

AVTOMATSKI VKLOPI: V primeru, da večkrat pozabimo vklopiti alarm, imajo vse centrale možnost programiranja sistema za samodejni vklop. Pri nastavitvi imamo proste roke, saj lahko avtomatski vklop nastavimo vsak dan ob točno določeni uri.

ŠTIRI ALI ŠEST MESTNA GESLA: za zmanjšanje možnosti zlorabe gesla je možno izbirati gesla dolžine šestih znakov. Pri uporabi gesel moramo biti pozorni, da ne izbiramo rojstnih dni ali podobnih gesel, ki bi jih lahko vlomilec uganil. Geslo omogoča vklop, izklop sistema in možnost dostopa do menijev nastavitvev. Tudi najenostavnejša centrala v družini DSC ima kar 32 različnih gesel. Raznolikost gesel je pomembna v primeru, ko je v sistemu več uporabnikov, saj lahko vršimo kontrolo uporabnika. Vsaka uporaba posameznega gesla se zapiše v spomin dogodkov. V nadzornem centru tako vidijo, katero geslo je bilo uporabljeno. Geslo za programiranje sistema je ločeno od gesel uporabnikov in ne omogoča vklopa ali izklopa sistema. Serviserjevo geslo se zapiše v programski zapisnik, da pri servisiranju ne pride do zapletov. Programski zapisnik je dokument, v katerega monter vpisuje parametre, ki jih je nastavil za določen protivlomni alarmni sistem.

ESCORT MODUL: Z uporabo modula ESCORT lahko vklopimo sistem na daljavo, pregledamo alarme v spominu, prožimo izhode PGM, izklopimo sistem in vklapljammo in izklapljammo druge storitve. Modul spremeni katerikoli tonski telefon v tipkovnico alarmnega sistema. Če smo na dopustu ali kjerkoli drugje, lahko preprosto preverimo stanje sistema.

BREŽIČNE RAZŠIRITVE: Vsako alarmno centralo DSC lahko nadgradimo z modulom za sprejem brezžičnih signalov in postavimo sistem brez ožičenja.

PC-LINK: Z uporabo posebnega priključnega kabla, imenovanega PC-link, lahko sistem popolnoma programiramo z uporabo računalnika in programske opreme DLS-3.

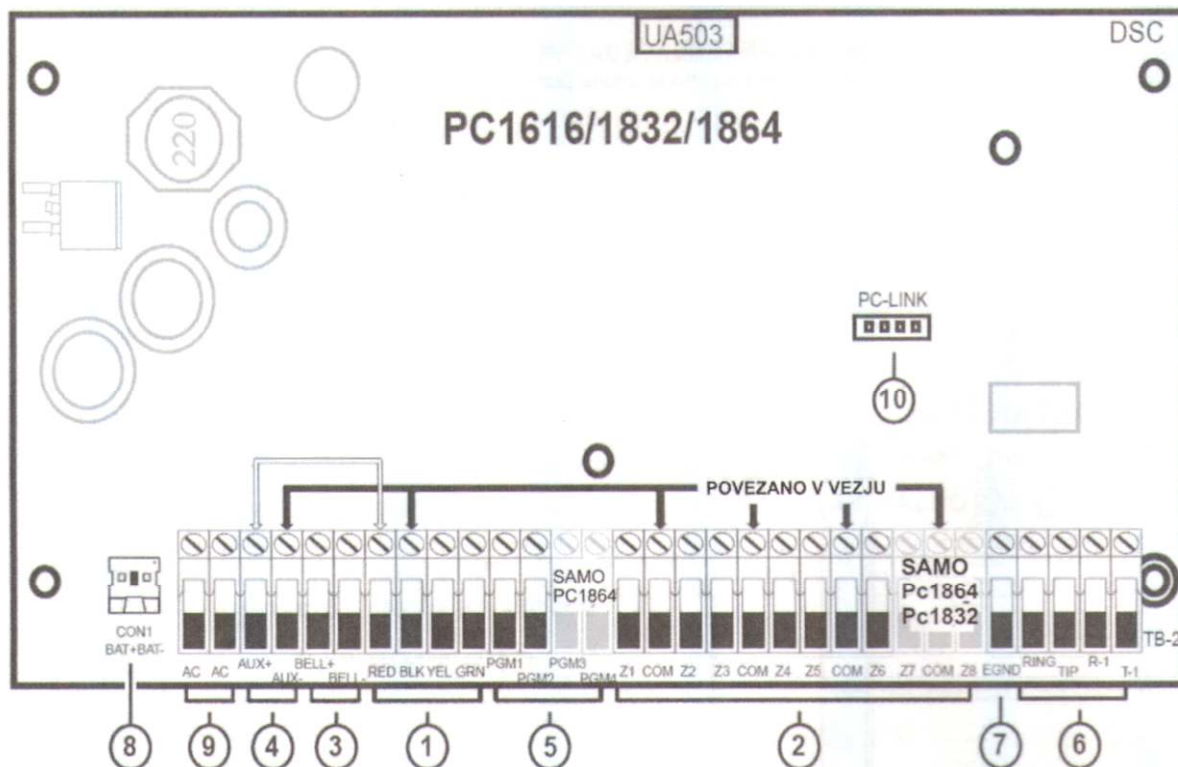
6.2.1. Vezalna shema alarmne centrale DSC

Na sliki 20 vidimo priključke alarmne centrale DSC serije new Power. Opis centrale sem razdelil na 10 točk.

Temperaturno območje delovanja alarmne centrale je med 0 °C in 49 °C, tako da centralo ne moremo imeti postavljeno zunaj hiše. To ne bi bilo pametno tudi iz vidika varnosti, saj je centrala vlomilcem bolj dostopna. Napajanje centrale dobimo iz transformatorja, ki ima izhodno napetost 16 VAC / 40 VA. Transformator je električna naprava, ki pretvarja električno energijo pri visoki napetosti v električno energijo pri nizki napetosti, ali obratno, kjer želimo dobiti iz višje napetosti nižjo. Na primarno stran transformatorja priključimo omrežno napetost 230 VAC 50 Hz. Iz sekundarne strani transformatorja pa pripeljemo napetost na številko devet na sliki 20, na priključka AC.

Ko priključimo omrežno napajanje ne smemo pozabiti na ozemljitev centrale in ozemljitev kovinske omarice. Rumeno/zeleno žico iz električne omarice priključimo na številko 7, na priključek EGND. Kovinsko ohišje ozemljimo s pomočjo vijaka in matice. Priključek

pričvrstimo tako, da barvo ohišja oluščimo in tako dobimo dober kontakt z ohišjem, kar pomeni dobro zaščito.



Slika 20: Priključki centrale PC1616 / 1832 / 1864 [6].

Opis ostalih priključkov alarmne centrale [12]:

KEYBUS (RED, BLK, YEL, GRN): štiri žična povezava, ki je potrebna za komunikacijo med alarmno centralo, tipkovnicami ter ostalimi moduli. Priključki si morajo slediti enako kot pri centrali (rdeča, črna, rumena, zelena) (točka 1). Priključek BLK je v vezju centrale povezan s priključkom AUX-, priključek RED pa na AUX+ (napajanje V_{SS} in V_{DD}).

PODROČJA (Z1 do Z8): osem možnih področij za priključitev senzorjev. Poljubno področje priključimo med kontaktom Z1 in COM, naslednje področje pa med Z2 in COM. Tako nadaljujemo do osmega področja (točka 2).

COM: negativni priključek področja (točka 2).

VEZAVA SIRENE (BELL+ in BELL-): izhod za sireno zagotavlja tokovno obremenitev do 700 mA. Če izhoda ne uporabljamo, ga nadomestimo z uporom vrednosti 100 Ω med oba priključka. Tako preprečimo obvestilo o napaki, če izhoda ne uporabljamo (točka 3).

NAPAJANJE (AUX+ in AUX-): priključka nam zagotavljata dodatno napajanje modulov, senzorjev, relejev in tipkovnic. Celotna poraba tipkovnic, PGM izhodov in AUX ne sme presegati 700 mA. Če skupna poraba presega omenjeno porabo, je potrebno uporabiti dodatni napajalnik (PC5200 ali PC5204). Izhodna napetost izhoda AUX je med 11.1 VDC do 12.6

VDC /700 mA. Delovna napetost senzorjev, tipkovnic in ostalih modulov pa je 9.5 VDC – 14 VDC (točka 4).

IZHODI PGM (PGM1, PGM2, PGM3 in PGM4): možni dodatni izhodi za delovanje alarmnega sistema. Izhod PGM ob določenem izpolnjenem dogodku sklene priključek na maso in ostane sklenjeno tako dolgo kot traja dogodek (točka 5).

TELEFON (RING, TIP, R-1 in T-1): Dovod telefonsko linije priključimo na priključka TIP in RING. Če imamo dodatni telefon ga priključimo na priključka R-1 in T-1 (točka 6).

AKUMULATOR (BAT+ in BAT-): Pod točko 8 imamo priključek za akumulator, ki nam omogoča delovanje protivlomnega alarmnega sistema tudi v primeru izpada električne energije. Priporočeni akumulatorji za alarmni sistem DSC so DSC BD4-12 napetosti 12VDC / 7Ah. Maksimalen delovni tok za kapaciteto 7 Ah je 700 mA. Glede na porabnike moramo izbrati primerno kapaciteto akumulatorja. Kapaciteta akumulatorja se z leti zmanjšuje, nanjo pa vpliva tudi kolikokrat se akumulator sprazni in napolni. Kapaciteta akumulatorja kaže količino električne energije, ki jo akumulator oddaja v določenem časovnem obdobju dokler akumulator ne doseže 1,75 V po celici oz. 10,5 V (velja za 12 V akumulator). Po definiciji je akumulator elektrotehnična naprava za shranjevanje električne energije na posreden način preko kemične energije. Priporočljivo je, da akumulator zamenjamo vsakih 3 do 5 let.

6.3. Primerjava tipkovnic proizvajalca DSC

Pri podjetju DSC so razvili nove tipkovnice serije new Power, ki jih odlikuje modern izgled. Na sliki 21 je prikazana trenutno najnovejša in najboljša tipkovnica LCD PK5500 proizvajalca DSC. Glavna prednost pred drugimi tipkovnicami je njen zaslon LCD. Na zaslon se lahko izpisuje besedila v dveh vrsticah, skupaj do 32 znakov.



Slika 21: Zunanja oblika tipkovnice LCD PK5500 [11].

Lastnosti tipkovnice LCD PK5500:

- možen prikaz 64 področij,
- vgrajenih osem jezikov (tudi slovenščina),
- prikaz stanja particij,
- nastavljiv vnos do 32 znakov za opis področij, particij in drugih izpisov na tipkovnici,
- modern izgled,
- večje tipke,
- pet funkcijskih tipk,
- enostavno programiranje datuma in časa,
- vhod/izhod na tipkovnici, ki lahko deluje kot področje ali programabilni izhod,
- nova ikona za prikaz napajanja,
- enostaven uvod kablov,
- zaščita s sabotažnim stikalom (tamper stikalo),
- ločene urgentne tipke,
- nastavitev zvoka indikacije po področju,
- nastavljiva osvetlitev in kontrast,
- nastavljiva jakost piskača,
- tipkovnica RKF5500 ima enake funkcije in integriran brezžični sprejemnik za 32 področij.

Na sliki 22 levo je prikazana preprostejša tipkovnica LCD ICON PK5501 desno pa tipkovnica LED PK5516.



Slika 22: Tipkovnica LCD ICON PK5501 (levo) in tipkovnica LED PK5516,(desno) [16].

Kot vidimo je tipkovnica protivlomnega sistema lahko preprosta z signalizacijo LED diod (brez zaslona) ali z zaslonom LCD ICON, preko katerega dobimo vse potrebne informacije o stanju alarmnega protivlomnega sistema. Za uporabnika je še posebej veliko lažje delati z tipkovnico LCD, saj nam ob morebitnem odprtem področju na zaslon napiše za katero področje gre.

Vrsta tipkovnice je predvsem pomembna pri programiranju oziroma nastavljanju lastnosti alarmnega sistema, manj pa pri samem delovanju sistema. Na voljo imamo tipkovnice LED,

LCD ICON in LCD (tabela 11). Najbolj primerna je LCD, ki je tudi najdražja. Pri tipkovnici LCD in LCD ICON natanko vidimo kaj vpisujemo, saj se vnosi sproti izpisujejo na zaslon LCD. Ko vstopimo v programiranje razdelka nam tipkovnica prikaže status, odvisno od tipa tipkovnice, ko vklopimo ali izklopimo določen funkcijo [6]:

TIP TIPKOVNICE	MOŽNOST VKLJUČENA	MOŽNOST IZKLJUČENA
LED	Področna dioda SVETI	Področna dioda NE SVETI
LCD ICON	Številka JE prikazana	Številka NI prikazana
LCD	Številka JE prikazana	Prikazan JE presledek

Tabela 11: Primerjava tipkovnic glede na prikaz stanja.

V tabeli 12 imamo podane primerjave lastnosti tipkovnic serije New Power proizvajalca DSC [11]:

Osnove lastnosti	PK5500	PK5501	PK5516	PK5508	LCD5511	LED5511Z	PC5508Z
Način prikaza	LCD/črke in številke	LCD/ikone in številke	LED diode	LED diode	LCD/ikone in številke	LED diode	LED diode
Število področij	64	64	16	8	64	8	8
Število particij	8	8	8	8	8	2	2
Število funkcijskih tipk	5	5	5	5	4	4	5
Funkcijske tipke za hitri izbor	DA	DA	DA	DA	NE	NE	DA
Urgentne tipke za hitri izbor	DA	DA	DA	DA	NE	NE	DA
Dvojne urgentne tipke	NE	NE	NE	NE	DA	DA	DA
Velikost tipk	Velike	Velike	Velike	Velike	Zelo velike	Zelo velike	Zelo velike
Ikona za prikaz napajanja	DA	DA	DA	DA	NE	NE	NE
Vgrajen senzor temperature	DA	DA	DA	DA	DA	NE	NE
Vhod na tipkovnici, ki lahko deluje kot področje	DA	DA	DA	DA	DA	DA	DA
Programabilni izhod	DA	DA	DA	DA	DA	NE	NE
Vezava z dvojnim uporom	DA	DA	DA	DA	NE	NE	NE
Programiranje časa	DA	NE	NE	NE	NE	NE	NE
Nastavitev osvetlitve	DA	DA	DA	DA	NE	NE	NE

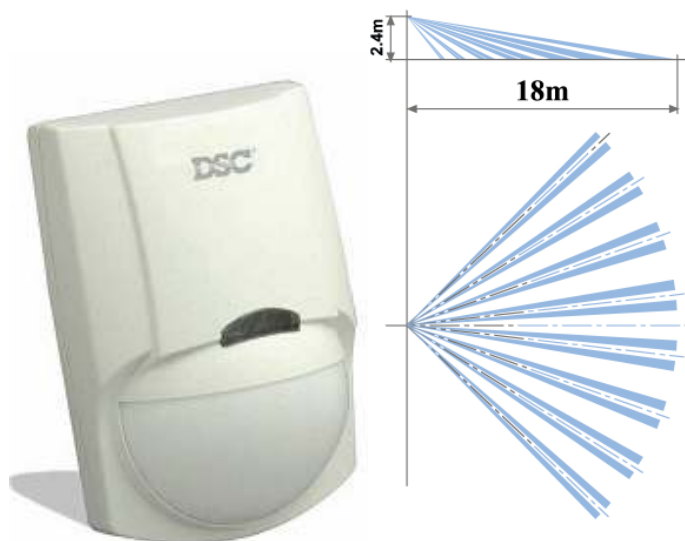
Nastavitev jakosti piskača	DA	DA	DA	DA	DA	DA	DA
Nastavitev zvoka indikacije	DA	DA	DA	DA	DA	NE	NE
Barva ohišja	Bela/črna	Bela/črna	Bela/črna	Bela/črna	Bela	Bela	Črna
Zasteklitev	Trdo	Trdo	Trdo	Trdo	Mehka	Mehka	Mehka
Pogled	Ležeče	Ležeče	Ležeče	Ležeče	Pokončno	Pokončno	Ležeče
Vgrajen RF sprejemnik	NE	NE	NE	NE	NE	NE	NE
Preprosta vgradnja	DA	DA	DA	DA	NE	NE	NE
Žični kanal	DA	DA	DA	DA	DA	DA	NE
Sabotažno stikalo	DA	DA	DA	DA	DA	DA	DA

Tabela 12: Primerjava lastnosti tipkovnic serije New Power pri DSC [11].

6.4. Primerjava senzorjev proizvajalca DSC

Serija senzorjev LC

Senzorji iz serije LC proizvajalca DSC nam nudijo zanesljivo zaščito za vsak prostor. Zanesljivost v preprečevanju lažnih alarmov se kaže v štirih senzorjih (vgrajenih v enega) in v posebej za ta namen razviti elektroniki. Omogočajo nam tudi nezaznavanje spodnje dela diagrama pokritja senzorja, to pa je namenjeno predvsem domačim živalim do 25 kg. Učinkovito zaznavanje sprememb je odvisno od zmožnosti senzorja pri zaznavanju vlomilca. DSC senzorji zaznajo vlomilca s pomočjo digitalnega procesiranja signala. DPS zagotavlja boljšo analizo signala in zmanjšanje vplivov na zaznavanje zaradi ojačitve, šuma, motenj ali delitve signala. Omogočajo tudi daljši domet od običajnih senzorjev zaradi okroglo oblikovane leče. Vsi senzorji imajo tudi možnost zaščite proti sabotaži z vgrajenim stikalom [11]. Spodaj na sliki 23 levo je prikazan infrardeči senzor LC-100PI, desno pa je prikazan njegov diagram pokritja. Polje pokritja senzorja je 18x18 m.



Slika 23: Notranji infrardeči senzor premika LC-100PI (levo) in diagram pokritja (desno) [11].

Serijska LC nam nudi tudi senzorje z dvojnimi delovanji, kateri imajo poleg IR senzorja tudi MW senzor. Poleg obeh načinov detekcije imamo na razpolago tudi "antimasking zaščito". Ta nam zagotavlja zaščito pred neželenimi približevanji in maskiranjem senzorja že pri razdalji 0,8 m. S stikalom v notranjosti senzorja lahko nastavimo občutljivost zaznavanja prekrivanja. Senzor omogoča občutljivost zaznavanja prekrivanja pri 0,4 m ali pri 0,8 m. Prav tako lahko z potenciometri nastavljamo tudi občutljivost IR in MW senzorja.

Efektivno območje detekcije senzorja je območje, kjer se IR in MW zaznavanje križata. Za pomoč pri postavitvi senzorja so nam na razpolago tri diode LED, ki se prižigajo ob dogodkih. Rdeča dioda LED gori med alarmom, zelena v primeru IR spremembe in rumena v primeru MW spremembe.

Senzor loma stekla ACUITY

Senzor ima vgrajeno tehnologijo, ki mu omogoča, da razlikuje zvok loma stekla od drugih običajnih zvokov. Možnost razbitja stekla je možna povsod, kjer imamo okna, torej v poslovnih in stanovanjskih objektih. Z vgrajenim mikrofonom in naprednim digitalnim procesiranjem zvočnih signalov, nam omogoča učinkovito detekcijo loma stekla vseh poznanih tipov. Primeren je za vse vrste gradnje, saj ima možnost montaže na strop ali na steno.



Slika 24: Zunanji obliko senzorjev loma stekla Acuity proizvajalca DSC [11].

Lastnosti:

- izjemni frekvenčni razpon mikrofонов omogoča izvrstno zajemanja zvoka nizke jakosti z dometom 7,6 m,
- s stikali lahko izbiramo občutljivost,
- digitalna obdelava signala analizira zvok do najmanjšega detajla, kar omogoča večje občutljivosti senzorja in odpornost na lažne alarme
- visok nivo zaščite pred statično elektriko in praznjenjem
- izredna detekcija loma stekla vseh poznanih tipov uokvirjenih stekel vključno z večslojnimi, termopan armiranimi in kaljenimi stekli
- senzor se prilagaja spremembam v konstrukciji okvirjev, debelini stekla in akustičnosti prostora

Simulator razbitja stekla Acuity AFT-100

Za testiranje delovanja senzorjev loma stekla uporabljamo simulator. Simulator ustvarja zvočne vzorce loma uokvirjenega ali kaljenega stekla. Če nam s simulatorjem vzbujani senzor sproži alarm pomeni, da senzor deluje. V simulator je vgrajen 7,62 cm velik zvočnik, ki natančno reproducira območje frekvenc, ki jih ustvari razbitje stekla. Simulator loma stekla je prikazan na sliki 25.



Slika 25: Simulator loma stekla AFT-100.

6.5. Razširitveni modul za dodatnih 8 področij PC5108 proizvajalca DSC

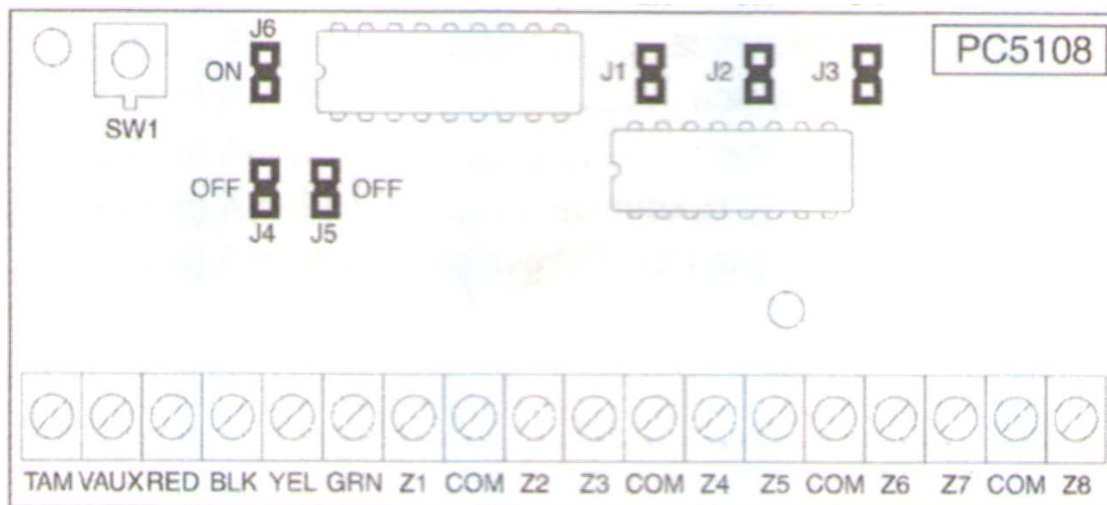
Razširitveni modul nam služi za povečanje področij centrale. Če imamo alarmno centralo s 6 področji in imamo v hiši 14 senzorjev, moramo dodati razširitveni modul. Modul nam omogoča razširitev sistema v korakih po 8 področij. Pri razširitvi moramo paziti koliko

razširitvenih področij nam omogoča alarmna centrala. Modul je kompatibilen z naslednjimi alarmnimi centralami: PC5010, PC5015, PC5020, PC1864, PC1832 in PC1616. Modul se lahko nahaja v istem ohišju kot alarmna centrala ali pa je postavljen v svojem ohišju. Različne razširitvene module ne smemo uporabljati v enem sistemu.

Za dodelitev posameznih področij je potrebna pravilna izbira stikal (jumperjev) J1, J2 in J3, ki so prikazani na sliki 26. Opis dodelitve področij pa je opisan v tabeli 13. Kot vidimo imamo tri stikala kar nam omogoča osem možnih kombinacij. Če so vsa stikala sklenjena, je modul onemogočen. Če imamo samo en razširitveni modul, omogočimo področja od devet do šestnajst tako, da sklenemo stikali J2 in J3, stikalo J1 pa razklenemo.

NASTAVITEV STIKAL MODULA			DODELITEV PODROČIJ
J1	J2	J3	
ON	ON	ON	PODROČJA ONEMOGOČENA
OFF	ON	ON	OMOGOČENA PODROČJA 09 ÷ 16
ON	OFF	ON	OMOGOČENA PODROČJA 17 ÷ 24
OFF	OFF	ON	OMOGOČENA PODROČJA 25 ÷ 32
ON	ON	OFF	OMOGOČENA PODROČJA 33 ÷ 40
OFF	ON	OFF	OMOGOČENA PODROČJA 41 ÷ 48
ON	OFF	OFF	OMOGOČENA PODROČJA 49 ÷ 56
OFF	OFF	OFF	OMOGOČENA PODROČJA 57 ÷ 64

Tabela 13: Notranja shema modula PC5108 za razširitev sistema [12].



Slika 26: Notranja shema modula PC5108 za povečanje področij sistema [12].

OPIS PRIKLJUČKOV:

TAM: uporaba varnostnega stikala (tamper stikalo), ki se sproži, če odpremo pokrov omarice vgrajenega modula. Stikalo, ki je normalno zaprto (NC – Normal Closed), povežemo med priključkoma TAM in BLK. Če stikala ne uporabimo naredimo kratek stik med TAM in BLK. S tem odpravimo javljanje napake alarmne centrale.

VAUX – za dodatno napajanje naprav, ki jih potrebujejo. Izhodna napetost je 12 V enosmerne napetosti (DC). Največji tok porabnikov ne sme presegati 100 mA. Pozitivni pol napajanja

priključimo na VAUX, negativni pol pa na BLK ali na katerikoli priključek COM. V vezju so BLK in vsi priključki COM povezani med seboj.

Priključke **KEYBUS (RED, BLK, YEL, GRN), Z1 do Z8, in COM** uporabljamo enako kot pri alarmni centrali.

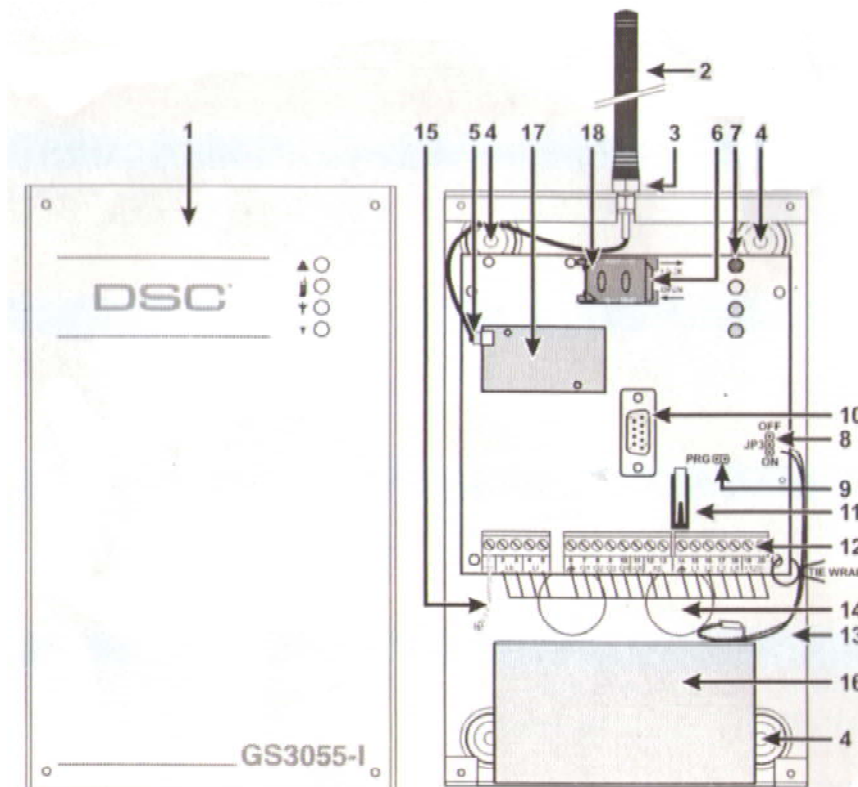
6.6. Univerzalni brezžični alarmni komunikator GSM/GPRS GS3055-I proizvajalca DSC

GS3055-I je univerzalni brezžični alarmni komunikator, ki deluje v omrežju GSM. Zagotavlja nam dodaten način komunikacije v primeru, ko telefonske linije nimamo na razpolago ali v primeru prekinjene linije. Prekinitev telefonske linije lahko povzroči strela in strukturna ali namerna sabotaza. V primeru sproženega alarma komunikator izvede povezavo na PSTN telefonsko linijo. Če povezava ne uspe, se komunikator poveže na omrežje GSM ter pošlje signal na varnostni nadzorni center ali na drugo telefonsko številko.

Lastnosti komunikatorja so [15]:

- simulira telefonsko linijo,
- avtomatični vklop v omrežje GSM v primeru prekinjene zemeljske linije,
- združljiv s katerokoli alarmno centralo, ki komunicira z uporabo formata CONTACT ID,
- poročilo o dogodkih,
- sprejema in oddaja prihajajoče in odhajajoče klice,
- indikator signala GSM (4 statusne LED diode prikazujejo moč signala in delovanje komunikatorja),
- vgrajeni 4 programabilni vhodi,
- 4 programabilni izhodi (odprti kolektorji),
- vgrajen skupaj z 12 V / 1,2 Ah baterijo,
- zaščita s sabotaznim stikalom (tamper stikalo),
- SMS funkcija pozivnika omogoča pošiljanje 13 predhodno nastavljenih sporočil v primeru sproženega alarma,
- za SMS funkcijo je na voljo 8 telefonskih števil,
- 95 telefonskih števil lahko sproži programabilne izhode,
- GPRS komunikacija je združljiva s sprejemnikom v varnostno nadzornem centru,
- napajalna napetost: 9 -14 VDC,
- tokovna poraba v mirovanju je 125 mA,
- tokovna poraba v uporabi (prenos signala) je 450 mA,
- paralelno sta lahko na LI priključeni 2 napravi, največja upornost zanke med dvema napravama pa je 1 k Ω ,
- temperaturno območje je med 0 °C in 50 °C,
- dimenzije naprave so 138 x 224 x 55 mm,
- teža (brez baterije) je 900 g.

6.6.1. Zgradba komunikatorja GSM/GPRS GS3055-I



Slika 27: Zgradba komunikatorja GSM/GPRS GS3055-I proizvajalca DSC [15].

Na sliki 27 lahko vidimo zgradbo komunikatorja GSM. Pod točko 1 je kovinsko ohišje, ki varuje notranji del pred mehanskimi poškodbami. Komunikator GSM mora biti vgrajen v notranjosti stavbe, signal GSM pa mora biti dostopen. Izogibati se moramo vlažnim prostorom ter postavitvi naprave preblizu radijskih sprejemnikov in podobnih naprav. Pod točko 2 imamo vgrajeno anteno GSM, pod točko 4 pa imamo pripravljene odprtine za vijake, kjer lahko napravo fiksno pritrdimo.

Ko napravo in anteno pritrdimo, priključimo anteno na modul GSM (točka 17). Kartico SIM vgradimo v držalo (točka 6) pred tem pa moramo na kartici izklopiti zahtevano kodo PIN pri vklopu telefona. Nato priključimo baterijo (točka 8) in priključimo napajanje enosmerne napetosti na priključka +/- 12 V. Zatim vključimo centralo in počakamo, da se delovanje naprave vzpostavi. Če sveti samo spodnja zelena dioda LED (točka 6) je signal dober, če pa svetita obe zeleni diodi LED pa je signal optimalen.

Če nam spodnja zelena dioda LED utripa pomeni, da ni zagotovljen dober signal. Napravo moramo premakniti in ponovno vzpostaviti, dokler dioda LED ne začne svetiti. Naprava ima poleg dveh zelenih diod LED tudi rdečo in rumeno. Rdeča dioda LED sveti v primeru napake. Rumena pa se prižge, ko naprava preklopi na omrežje GSM (v primeru sabotaže stacionarne telefonske linije). Ko zaključimo povezave (točka 12) napravo zapremo in zaščitimo s

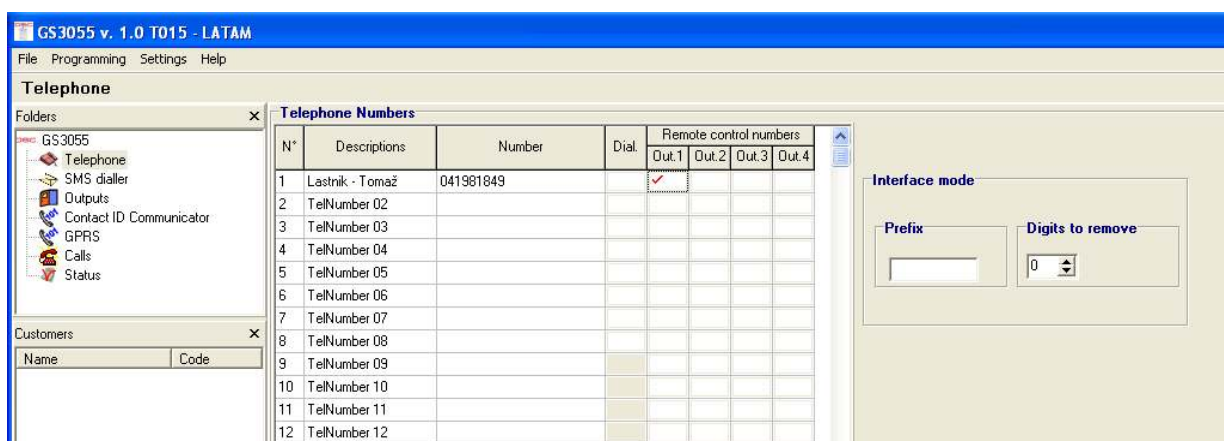
6.6.3. Programiranje komunikatorja

Komunikator nastavljamo s pomočjo programskega vmesnika proizvajalca DSC. Ko začnemo s programiranjem, najprej generiramo novega uporabnika z ukazom File->New. Pod zavihkom Panel Type izberemo ime naprave, v našem primeru je to GS3055. Pod opcijo Settings->Serial Ports izberemo serijski vhod računalnika, na katerega smo priključili napravo. Preden pošljemo podatke v napravo, jih moramo shraniti z ukazom File->Save.

Možno je tudi programiranje naprave iz oddaljene lokacije (Remote programming). Ko spremenimo uporabniške podatke, s kratkim sporočilom SMS pošljemo zahtevo za oddaljeno programiranje (#KODA#*PRG*). Z ukazom SMS #KODA#** pa povezavo zaključimo.

TELEFONSKI IMENIK (TELEPHONE PAGE)

Telefonski imenik lahko hrani do 95 telefonskih števil. Za prvih osem lahko uporabljamo funkcijo pošiljanja kratkih sporočil SMS.



Slika 29: Pregled telefonske strani v programskem vmesniku GS3055.

Pod stolpec Description vpišemo ime uporabnika telefonske številke. Za ime lahko vpišemo do 20 alfanumeričnih znakov. V polje Number vpišemo telefonsko številko, dovoljene pa so samo številke od 1 do 9 in znak +. Pod stolpec Dial vključimo polja, s katerim označimo katere telefonske številke bodo sprejemale opozorilna sporočila ob določenem dogodku. Dogodke nastavljamo na strani SMS dialler. Pod stolpcem Remote control numbers označimo polja ter s tem definiramo telefonske številke, ki bodo lahko vklapljale izhode (O1, O2, O3 in O4) preko telefona. Tukaj lahko vidimo, da lahko z eno telefonsko številko vklapljamo vse 4 izhode. Prav tako pa lahko več telefonskih števil vklaplja en izhod.

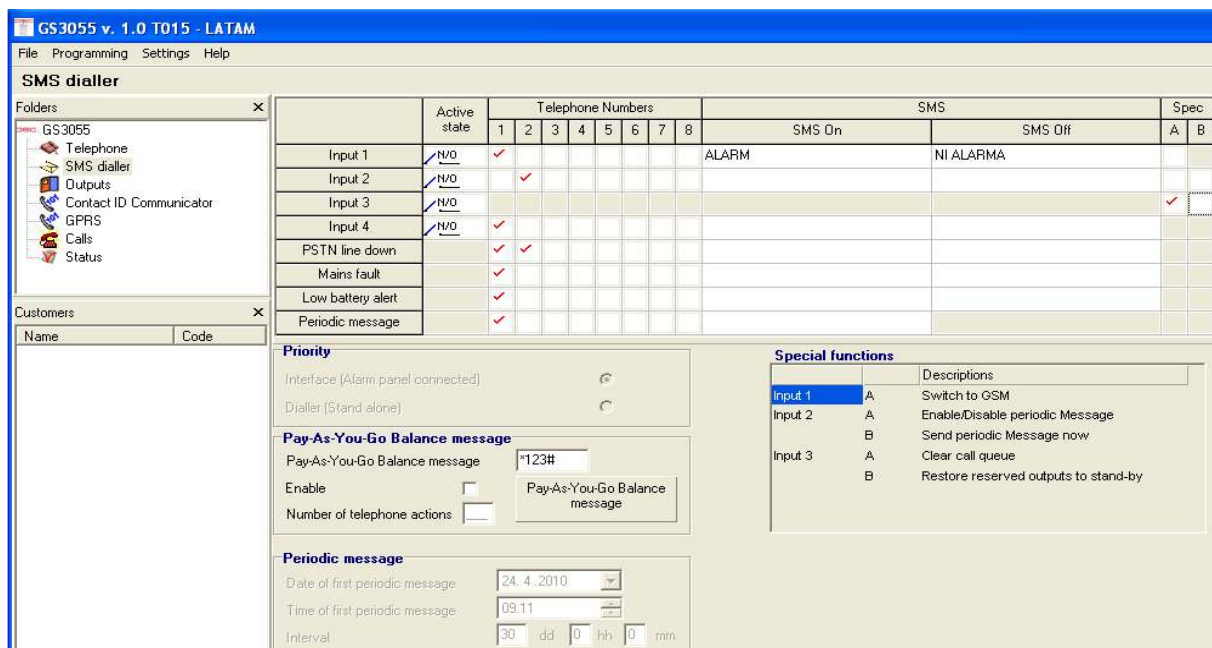
IMENIK KRATKIH SPOROČIL (SMS DIALLER PAGE)

Komunikator lahko pošilja kratka sporočila osmim telefonskim številkam, ki so shranjene v telefonskem imeniku.

Kot vidimo na sliki 30, lahko izberemo različne dogodke, ki ob določeni spremembi pošljejo kratko sporočilo na izbrane telefonske številke:

- sprememba napetosti na vseh 1,2,3,4 (Input 1,2,3,4). V stolpcu Active state določimo, ali bo vhod aktiven v visokem ali nizkem stanju.

- test stacionarne telefonske linije (PSTN line down),
- napaka napajanja (Mains fault),
- obvestilo o prazni bateriji (Low battery alert),
- periodično sporočilo (Periodic message).

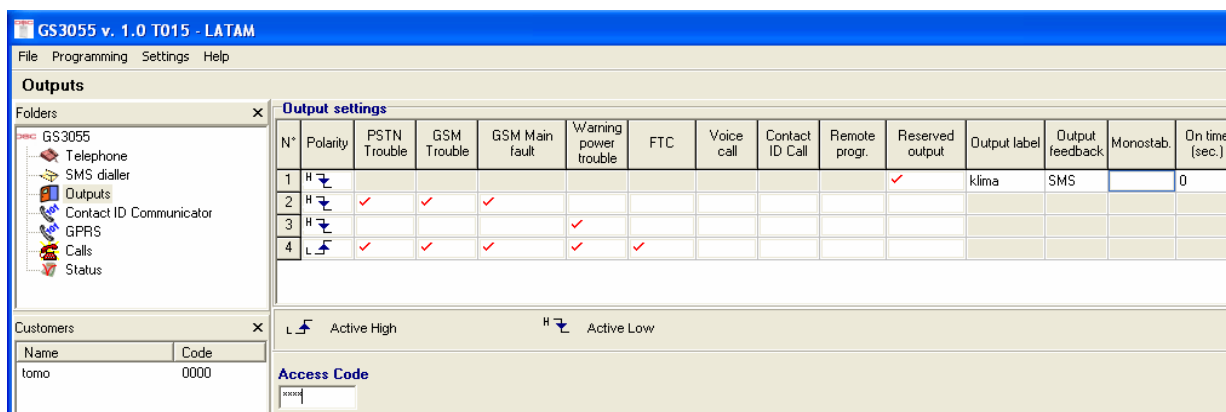


Slika 30: Imenik kratkih sporočil v programskem vmesniku GS3055 (SMS dialler page).

Pod stolpec SMS (slika 30) napišemo dve pregledni sporočili z opisom določenega dogodka. V stolpcu Spec lahko definiramo nekatere vgrajene specialne funkcije za prve tri vhode. Pri izbiri pošiljanja periodičnih sporočil (Periodic message), lahko nastavimo čas in datum prvega sporočila in interval med poslanimi sporočili. To lahko izkoristimo za testiranje komunikatorja. Če v trenutku preneha delovati glavno napajanje (12 VDC) in baterija, moramo ponovno nastaviti periodična sporočila.

IMENIK IZHODOV (OUTPUT PAGE)

Tukaj lahko nastavimo nastavitve izhodov. Izhodi so definirani kot normalno odprta stikala in so sklenjena na maso ob aktivaciji izhoda. Porabnik se priključi na enega izmed izhodov in pozitivni pol napajanja.



Slika 31: Imenik izhodov v programskem vmesniku GS3055 (Outputs page).

Napravo lahko nastavimo tako, da ima izhode nastavljene kot avtomatične (Automatic outputs) ali kot oddaljen dostop (Remote control outputs). Avtomatični vklop izhoda PGM se aktivira, če se zgodi kateri od naslednjih dogodkov:

- napaka stacionarne telefonske linije (PSTN trouble),
- napaka omrežja GSM (GSM trouble),
- napaka modula GSM (GSM main fault),
- napaka glavnega napajanja ali baterije (Warning power trouble),
- FTC, prihajajoč klic (Voice call),
- priklop daljinskega programiranja (Remote programming).

Avtomatični izhod je vklopljen toliko časa dokler ni odpravljena napaka ali dejanje.

Če označimo polje v stolpcu Reserved output (rezerviran izhod) nastavimo izhod kot oddaljen dostop. Oddaljen dostop je lahko nastavljen kot BISTABILNI (izhod lahko vklopimo in izklopimo s sporočilom ali s klicem) ali kot MONOSTABILNI (izhod lahko samo vklopimo s sporočilom ali s klicem). Če hočemo, da je izhod monostabilen označimo polje v stolpcu Monostab, če pa hočemo, da je izhod bistabilen pa pustimo polje neoznačeno. Vsak rezerviran izhod lahko ob vklopu pošlje potrditveni sms ali klic. To nastavimo v stolpcu Output feedback.

VKLOP IN IZKLOP BISTABILNEGA IZHODA

Bistabilni izhod lahko vklopimo na dva načina:

1. Pošljemo SMS sporočilo na številko GSM komunikatorja. Najprej med znakoma # vpišemo kodo, ki jo nastavimo v polju Access Code. Nato napišemo opis izhoda, ki ga vpišemo v polje v stolpcu Output label. Nato sledi še oznaka za vklop (ON) ali izklop (OFF) izhoda.
Primer vklopa klimatske naprave v hiši bi izgledalo tako: # KODA#KLIMA=ON.
Primer izklopa klimatske naprave pa: # KODA#KLIMA=OFF
2. Izhod lahko vklopimo in izklopimo tudi s klicem iz telefonske številke nastavljene v telefonskem imeniku.

Monostabilni izhod lahko enako vklopimo na zgoraj navedena načina. Edina razlika je v tem, da ga nam ni treba izklopiti. Če ga ne izklopimo, bo izhod vklopljen za čas nastavljen v polju On time (Sec.).

7. Priprava za protivlomni alarmni sistem pri novogradnji

Pri postavitvi in izbiri alarmnega sistema je pomembno, da na to mislimo že pri novogradnji ali adaptaciji objekta. Tako lahko zmanjšamo stroške, saj ni potrebno naknadno vrtati in razbijati sten ter kable polagati v nadometne kanale. Ko je objekt končan in so vsi izvajalci z deli že končali, pride do veliko slabe volje in nepotrebnih stroškov, ko se odločimo za instalacijo protivlomnega sistema. Željo po vgradnji sistema moramo takoj povedati arhitektu, ki bo pripravil projekt arhitekture objekta. Ta bo prilagodil in uskladił pozicije posameznih elementov sistema in opremo. V sodelovanju s projektantom elektro instalacij pa se poskrbi, da so elementi vrisani tudi v projekt elektro instalacij. Ne glede na to kdaj se odločimo za nakup alarmnega sistema, moramo ob gradnji pripraviti cevi za postavitev sistema v prihodnje. Za pripravo se uporablja zaščitna rebrasta cev RBT, za polaganje v zid in beton premera $\phi 13,5$ ali $\phi 16$. Karakteristike RBT cevi za podometno instalacijo so [16]:

- material je temperaturno visoko odporen HDPE
- cev je oranžne ali druge barve,
- odpornost na pritisk: 320 N/5 cm pri 20 °C,
- odpornost na udarec: 2 J pri -5 °C,
- temperaturna obstojnost: -20 °C do +90 °C,
- odpornost na zunanje vplive: vodo, olje, gradbene materiale in korozijo,
- ni odporna na ogenj.

Če električno instalacijo postavljamo v votle pregradne stene in v zgradbe, kjer je predpisano neširjenje strupenih plinov v primeru požara, uporabljamo sivo RFS cev. Karakteristike sive RFS cevi za podometno instalacijo so [16]:

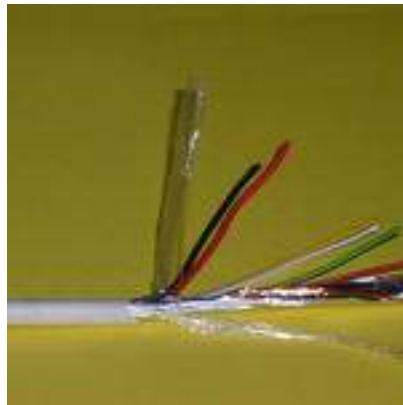
- material je temperaturno visoko odporen,
- cev je sive barve
- odpornost na pritisk: 125 N/5 cm pri 20 °C,
- odpornost na udarec: 1 J pri -5 °C,
- temperaturna obstojnost: -20 °C do +90 °C,
- odpornost na zunanje vplive: vodo, olje, gradbene materiale in korozijo,
- **odporna na ogenj.**



Slika 32: Siva cev RFS (levo) in oranžna cev RBT (desno) velikosti $\Phi 16$ [16].

Na sliki 32 sta prikazani cev RFS (levo) in cev RBT (desno). Pri uporabi zaščitnih cevi lahko kabel kadarkoli zamenjamo.

Za dovod električnega napajanja do centrale uporabimo kabel NYM-J 3x1,5, dovod pa pripeljemo iz električne omarice. Za povezavo med alarmno centralo in ostalimi napravami uporabljamo kabel, z oznako Licy 4x0,22+2x0,55 mm. Kabel je sestavljen iz štirih žic premera 0,22 mm, ki se uporabljajo za signale in dveh žic debeline 0.55 mm, ki se uporabljata za napajanje senzorjev. Oplet je oklopljen s posebno folijo za zaščito pred zunanjimi vplivi.



Slika 33: Kabel Licy za povezavo med alarmno centralo in ostalimi napravami [16].

Za povezavo med napravami lahko uporabljamo tudi kabel UTP (*Unshielded Twisted Pair*). UTP kabel je neoklopljen in vsebuje štiri medsebojno prepletene parice. Uporablja se za povezave v lokalnih omrežjih in v telekomunikacijah, vendar je primeren tudi za naš primer. Zaradi prepletenosti žil v kablu UTP se zmanjša presluh. Presluh je pojav, pri katerem se zaradi spreminjanja signala v eni liniji pojavi motilni signal v sosednjih linijah. Presluh je rezultat vpliva elektromagnetnega polja ene linije na sosednje linije, njegova velikost pa je odvisna od medsebojne induktivnosti in medsebojne kapacitivnosti linij. Pomembno je, da je presluh čim manjši.

Kabel UTP se v računalništvu uporabljajo za krajše razdalje, ker je poceni v primerjavi z optičnimi in koaksialnimi kabli. Kabli so primerni za uporabo v računalniških sistemih, merilnih in kontrolnih sistemih in v visokofrekvenčnih analognih prenosih. Zaključimo ga s konektorjem RJ-45, ki ga danes uporablja večina omrežnih naprav.

8. Primer izvedbe protivlomnega alarmnega sistema z uporabo naprav proizvajalca DSC

V praktičnem primeru sem pri novogradnji hiše pripravil in vzpostavil protivlomni alarmni sistem. Poleg alarmnega sistema sem pripravil in vzpostavil celotno električno omrežje, kar mi je zelo pomagalo pri montaži alarmnih enot, saj sem sam izvedel tako električno, kot tudi protivlomno napeljavo.

8.1. Napeljava in montaža protivlomnega alarmnega sistema

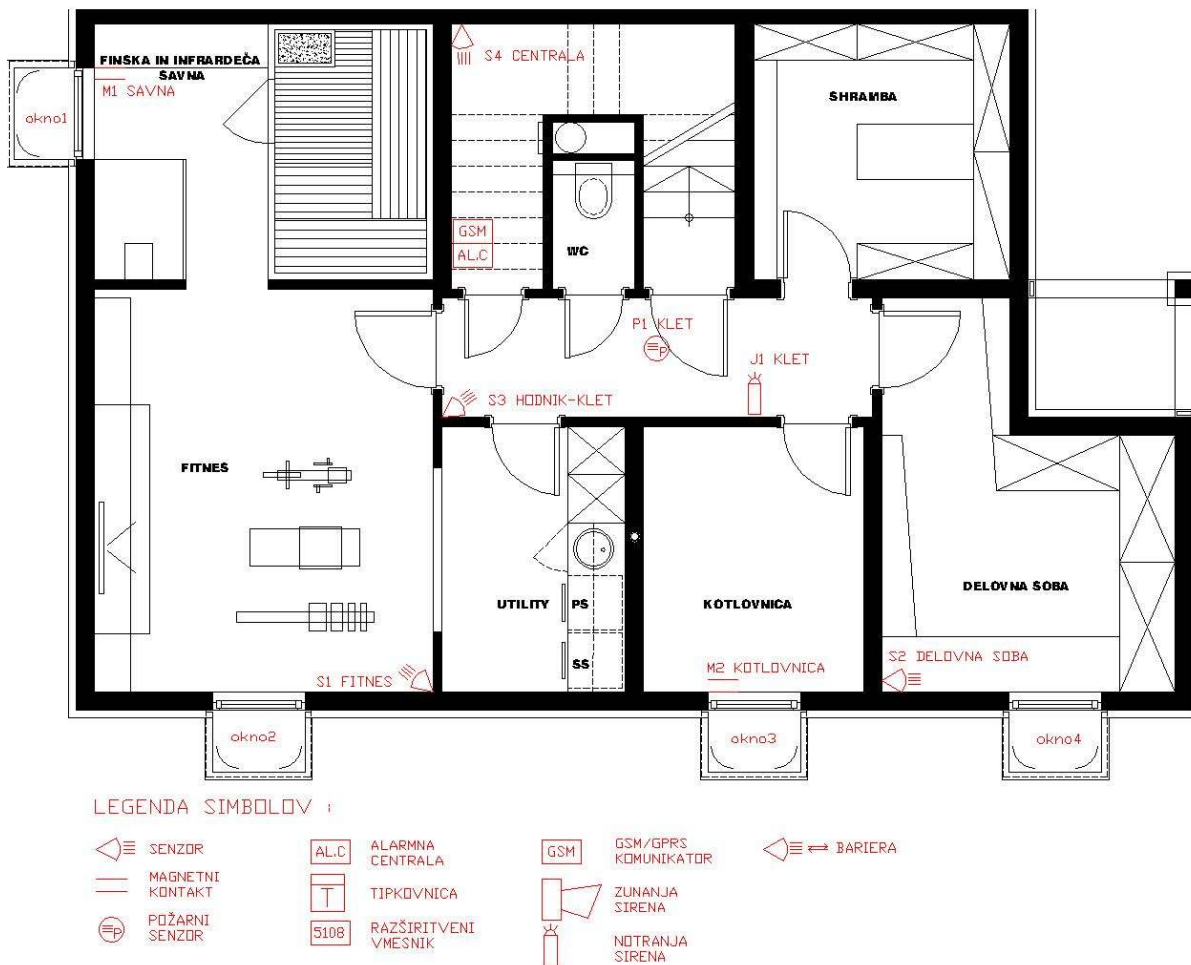
Objekt je razdeljen na tri nadstropja, kleti, pritličja in mansarde. S pomočjo programa AutoCAD Electrical 2009 sem ponazoril električne elemente (vtičnice, stikala in luči) in protivlomne elemente. Ker sem se osredotočil na protivlomni alarmni sistem, sem izklopil vse druge plasti v programu za boljšo preglednost slike. Pri postavitvi alarmnega sistema moramo poleg strokovnjaka za postavitve alarmnih sistemov upoštevati tudi želje in zahteve uporabnika.

8.1.1. Zaščita kleti

Ker v kleti na sliki 34 ni vhodnih vrat, je vstop od zunaj možen samo skozi posamezna okna. Alarmno centralo in komunikator GSM sem skrtil pod stopnice in tako omejil nepooblaščen dostop. Pri postavitvi komunikatorja GSM moramo biti pazljivi na dosegljiv signal, saj sistem s slabim sprejemom ne bi bil učinkovit. Glede na to, da je naprava v kleti, moramo testirati signal z zaprto omarico in zaprtimi vhodnimi vrati (simuliramo vsakodnevno delovanje). V primeru prešibkega signala moramo napravo postaviti višje v pritličje ali v mansardo. Alarmno centralo in komunikator GSM poleg sabotažnih stikal varujeta senzorja PIR S3 in S4. Senzor S3 ščiti tudi hodnik med posameznimi prostori in preprečuje prehod v zgornjo etažo. Okno1 pri savni je varovano z magnetnim kontaktom M1, saj varovanje s senzorji ni priporočljivo zaradi vlage in temperaturnih sprememb v prostoru. Senzor PIR S1 varuje vstop skozi okno2. Dodali smo notranjo svetlobno signalizacijo z bliskavico za dodatno opozorilo vlomilcu, da se je sprožil alarm. V kotlovnico je vstop možen skozi okno3, ki ga zaščitimo z magnetnim stikalom M2. V shrambi ni nobenega vhoda, zato nam tega prostora ni treba varovati. Vstop v shrambo pa vseeno varuje senzor na hodniku S3, če se vlomilec prebije skozi vse druge ovire. V delovni sobi senzor PIR S2 varuje nekatere vrednejše stvari in ostale pomembne dokumente. Za manjšo zaščito požara smo v hodniku postavili en dimni senzor P1. Vse senzorje PIR se za boljšo učinkovitost proti lažnim alarmom lahko zamenja z senzorji PIR&MW.

V kleti imamo 7 senzorjev (2 magnetna kontakta, 4 senzorje tipa PIR in 1 protipožarni senzor) in sabotažno stikalo, kar nam omogoča samo uporabo alarmne centrale brez razširitvenega modula. Izbrali smo alarmno centralo PC1864 DSC serije New Power. Lahko bi sicer uporabili alarmno centralo PC1616 ali PC1832, vendar je razlika v ceni tako majhna (manj

kot 15 €), da smo uporabili boljšo izmed teh. Centrala omogoča priklop osmih področij in štirih programabilnih izhodov. Tako nam bo eno področje ostalo za rezervo. Za boljšo alarmno centralo smo se odločili tudi zato, ker smo že pri gradnji pripravili instalacijo za garažo in manjši poslovni objekt, ki bo zgrajen v prihodnosti. Tako se bo lahko z enim sistemom upravljalo vsaj tri particije: hišo, garažo in poslovni objekt. Pri vgradnji sistema moramo vedno dobro premisliti, kako bo v prihodnosti. Če načrtujemo dodatno gradnjo ob obstoječem, je vedno dobro pustiti kakšno dodatno ožičenje do načrtovanega objekta ali pa enostavno pustimo samo prazno cev.

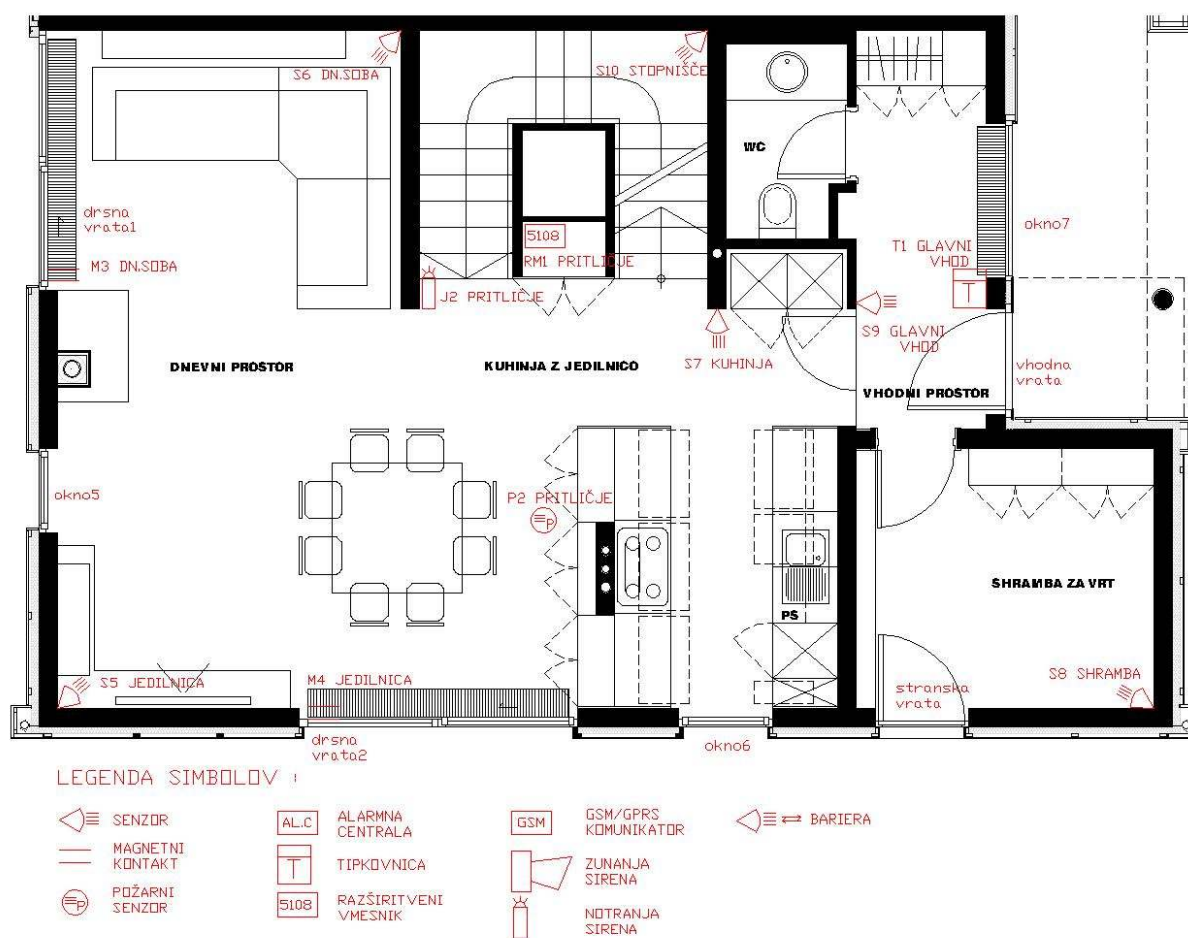


Slika 34: Tloris kleti z legendo protivlomnih simbolov.

V kleti ne potrebujemo tipkovnice, saj nimamo nobenega vhodnega prostora iz katerega bi prišli v hišo. Zato so vsi ti javljalniki vloma (senzorji in magnetni kontakti) definirani kot takojšnji alarm. Vsak senzor PIR ali PIR&MW je priključen na svoje področje (priključek Z_x) na alarmni centrali in je vezan z dvojnimi zaključnim uporom (DEOL). V pritličju in mansardi pa so javljalniki priključeni na področja razširitvenih modulov. Z DEOL vezavo smo rešili sabotažo vseh senzorjev. Sabotažno stikalo alarmne centrale in komunikatorja GSM pa priključimo na področje Z1 na sami centrali. Stikali priključimo zaporedno. S tem dosežemo, da nam centrala javi alarm pri odpiranju alarmne centrale ali komunikatorja GSM.

V primeru alarma bo sprožena sirena in prenos alarma na izbrane telefonske številke. Sirena je priključena na izhod PGM2, ki zagotavlja tokovno obremenitev 300 mA. Za prenos alarma smo uporabili komunikator GSM, ki simulira telefonsko linijo na alarmni centrali. Pri nastavljanju lastnosti alarmne centrale smo definirali tri telefonske številke, ki jih alarmna centrala s pomočjo komunikatorja GSM pokliče. Komunikator GSM lahko uporabimo tudi za sporočanje različnih dogodkov z SMS sporočili. Nastavimo lahko dve SMS sporočili, tako za vklop kot za izklop dogodka. Notranje sirene ali bliskavice J1, J2, J3 in zunanja sirena J4, imajo nalogo opozarjanja vlomilca in drugih, da se je sprožil alarm.

8.1.2. Zaščita pritličja



Slika 35: Tloris pritličja z legendo protivlomnih simbolov.

V pritličju na sliki 35 je bila predvidena zaščita vseh prostorov razen sanitarnega prostora. Vstop v hišo je možen preko vhodnih in stranskih vrat, preko obeh drsnih vrat in vseh oken. V prostoru med stopniščem je podometno vgrajen razširitveni modul za dodatnih osem področij RM1 z vgrajenim sabotajnim stikalom. Vhodna vrata in tipkovnico T1 varuje senzor S9, stranska vrata pa varuje senzor S8. Senzorja S5 in S6 varujeta dnevni prostor, obe drsni vrati in okno5. Celotni dnevni prostor nam že pokrije senzor S5 tako, da nam senzorja S6 ne bi bilo treba vgraditi. Vendar, če v primeru vstopa vlomilec razkrije varovalo M3, nam bo senzor S6 hitreje javil vlom kot senzor S5, ki ga prekriva kamin. Za dodatno zaščito smo zavarovali obe

drsnih vrati z magnetnima kontaktoma M3 in M4. Idealna postavitev senzorja za varovanje okna6 bi bila v desnem kotu pri oknu6, vendar zaradi visečih omaric v kuhinji ta postavitev ni možna, zato smo senzor za varovanje kuhinje in okna6 postavili na drugo primernejše mesto. Enako velja za senzor S9 pri glavnem vhodu, saj bi bilo primernejšo mesto v desnem kotu pri garderobnih omaricah. Za požarno varovanje smo se odločili za en dimni senzor P2 med kuhinjo in jedilnico, tako da varuje celotni prostor.

Pritličje varujemo s pomočjo 9 javljalnikov (4 senzorji tipa PIR, 2 senzorja tipa PIR&MW, 2 magnetna kontakta in 1 protipožarni senzor). Ker smo področja razširitvenega modula RM1 napolnili s sabotaznim stikalom modula in s 7 javljalniki, smo senzorja P2 in S10 priključili na razširitvene module v mansardi. Senzorja S5 in S6 sta tipa PIR&MW zaradi vgrajenega kamina v dnevni sobi. Ostali senzorji so lahko tipa PIR.

Ker je vstop v objekt možen iz dveh vhodov, morata biti senzorja S8 in S9 nastavljena z zakasnitvijo. Zakasnitev pomeni, da ima uporabnik na voljo določen čas za vklop in izklop sistema. Nastavljena vhodna zakasnitev je 30 sekund, izhodna pa 45 sekund. V primeru vstopa moramo v tem času priti do tipkovnice T1 in vtipkati geslo za izklop alarma. Če tega ne uspemo v 30 sekundah, se sproži alarm. Alarm se sproži tudi v krajšem času, če se poleg senzorja S9 aktivira tudi na primer senzor S7.

Najlažji vstop v hišo je preko obeh drsnih vrat, saj vlomilec vstopi z vrta takoj v dnevno sobo. Kot smo že omenili, smo nastavili dodatno zaščito z magnetnimi stikali, zaradi večjih steklenih površin pa bi lahko postavili tudi javljalnik loma stekla pri drsnih vratih 1, drsnih vratih2 in oknu 7.

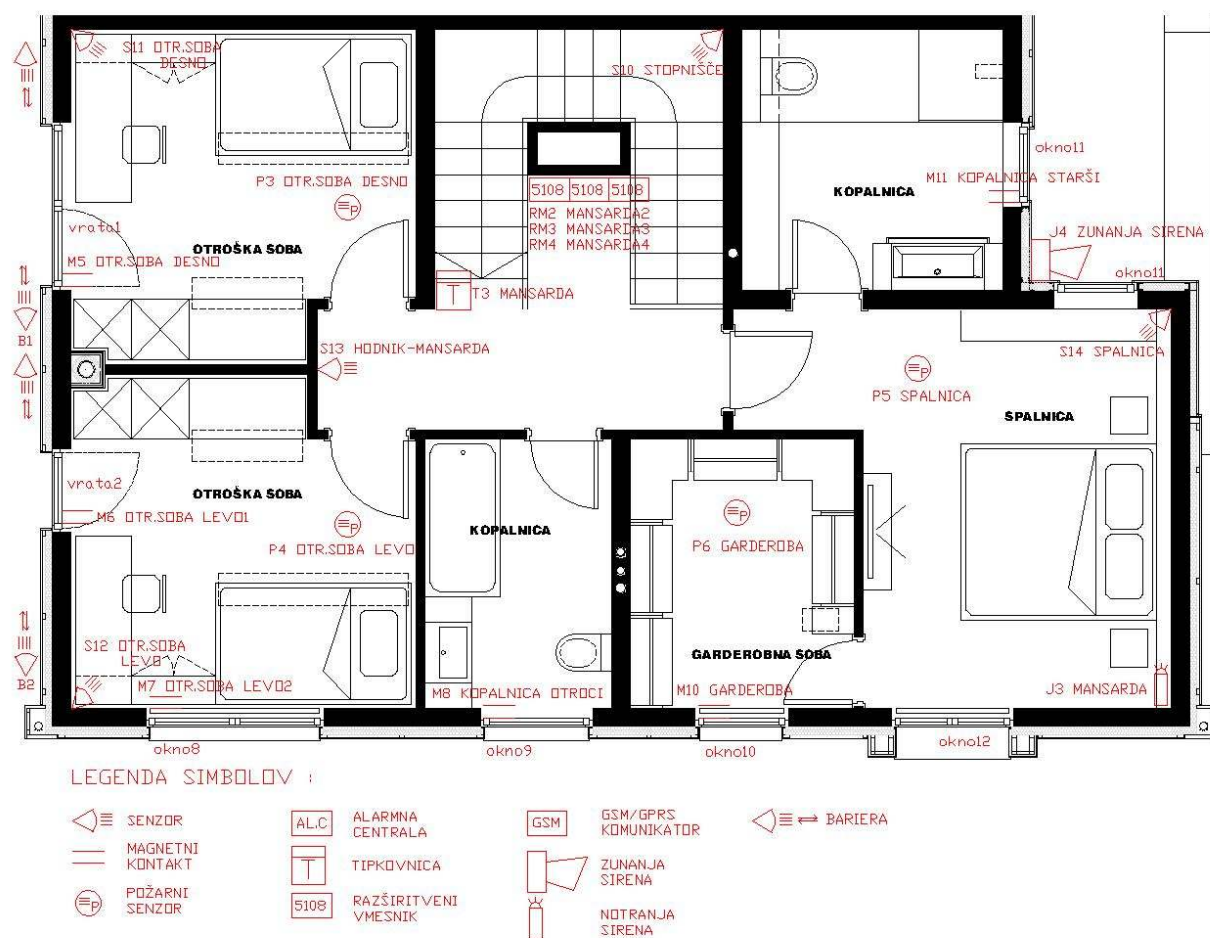
8.1.3. Zaščita mansarde

V mansardi na sliki 36 je bila predvidena zaščita vseh prostorov. Vstop v hišo je možen skozi balkonska vrata obeh otroških sob in skozi vsa okna v mansardi. Za vklop sistema (vklop nočnega varovanja) uporabimo tipkovnico T3. Senzorja S11 in S12 varujeta celotno sobo in vstopne točke v otroških sobah. Z magnetnimi senzorji M5, M6 in M7 varujemo odpiranje oken, z žarkovnimi barierami B1 in B2 pa vstop ali izstop z balkona. V obeh kopalnicah zaradi vlage zavarujemo okna z magnetnim kontaktom. Senzor S14 varuje prostor v spalnici ter vhod iz okna11 in okna12. Garderobno sobo zavarujemo z magnetnim kontaktom M10. V mansardi smo se odločili za večje število požarnih senzorjev zaradi otrok ter večje požarne nevarnosti. V nadstropju smo tako vgradili še en požarni senzor P7 (ni prikazan na slikah), ki dodatno varuje nadstropni prostor, v katerem so tudi zunanje enote klimatskih naprav. Na zunanji strani na najvišji točki imamo postavljeno zunanjo sireno J4.

Ker imamo v mansardi 17 senzorjev (6 magnetnih kontaktov, 5 senzorjev tipa PIR&MW, 2 barieri in 4 protipožarne senzorje), so med stopniščem podometno vgrajeni trije razširitveni moduli PC5108. Kot vidimo sta razširitvena modula RM2 in RM3 zapolnjena, pri RM4 pa imamo na voljo še 4 prikllope. Za KEYBUS komunikacijo med centralo in moduli potrebujemo samo en kabel od alarmne centrale. Med seboj pa povežemo ostale module

RM2, RM3 in RM4. Ta način nam prihrani polaganje kablov od vseh javljalnikov do alarmne centrale.

Varnostni sistem v mansardi ima dve funkciji. V primeru odsotnosti je to varovanje premoženja, v primeru prisotnosti (ponoči v spanju) pa nočno varovanje. Tako so vsi senzorji v mansardi S10, S11, S12, S13 in S14 nastavljeni kot nočno področje. Vsi ostali senzorji bodo kljub nočnemu vklopu sprožili alarm. Nočno varovanje lahko vklopimo iz katerekoli od dveh tipkovnic, vendar bomo to najlažje storili s tipkovnico T3, ki je postavljena v mansardi ravno zaradi nočnega varovanja. Vsi ostali senzorji so definirani kot področje, ki bo takoj sprožilo alarm (vsi magnetni kontakti in obe barieri). Pri teh nastavitvah se lahko družina nemoteno sprehaja po mansardi, ne da bi sprožila alarm.



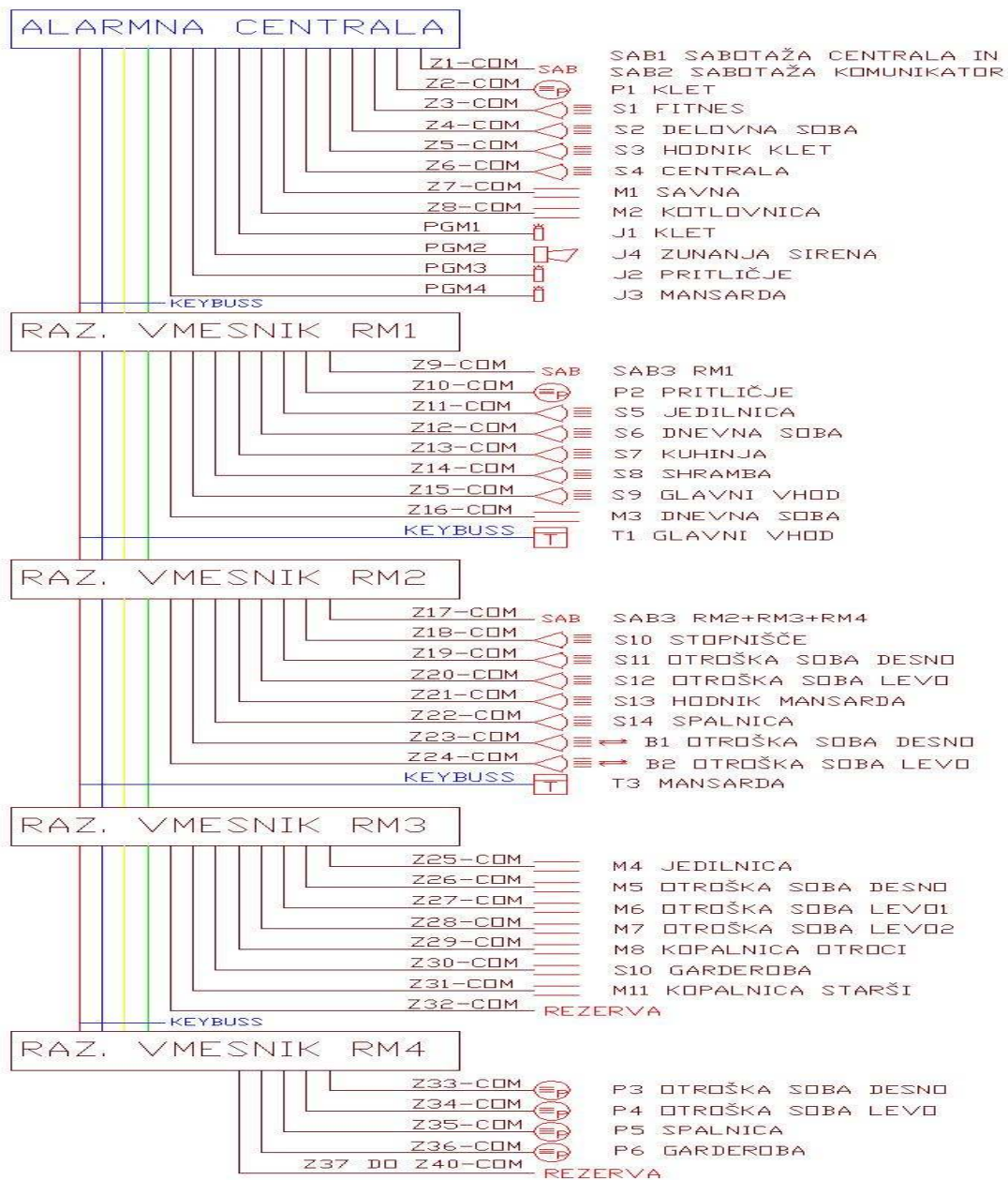
Slika 36: Tloris mansarde z legendo protivlomnih simbolov.

V obeh otroških sobah imamo zaradi varnosti otrok poleg nočnega varovanja s senzorjem vgrajena tudi magnetna kontakta pri vratih (M5 in M6) in bariere (B1 in B2). Tako smo lahko brez skrbi, da nam otrok ne bi zvečer ušel skozi vrata na balkon. Bariere so postavljene zato, ker ima vlomilec prelahak dostop do balkona. Bariere lahko postavimo tudi že prej pri zunanji ograji in tako vlomilcu preprečimo dostop na balkon in tako morebitno škodo, ki bi jo naredil.

Tip senzorja S13 je lahko notranji infrardeči senzor premika. Zaradi vgrajenih klimatskih naprav v obeh otroških sobah in spalnici morajo biti senzorji dvojne tehnologije zaradi temperaturnih sprememb, ki jih povzroča klima.

8.1.4. Popis materiala

Ker nas velikokrat pri tovrstnih instalacijah zanima cena, sem v tabeli 14 prikazal okvirne cene (maj 2010) naprav alarmnega sistema proizvajalca DSC za omenjeni objekt. Vse cene vključujejo DDV. Na sliki 37 pa sem ponazoril povezave alarmne centrale in razširitvenih modulov. Kot vidimo imamo na razpolago še veliko rezervnih priključkov na razširitvenih modulih.



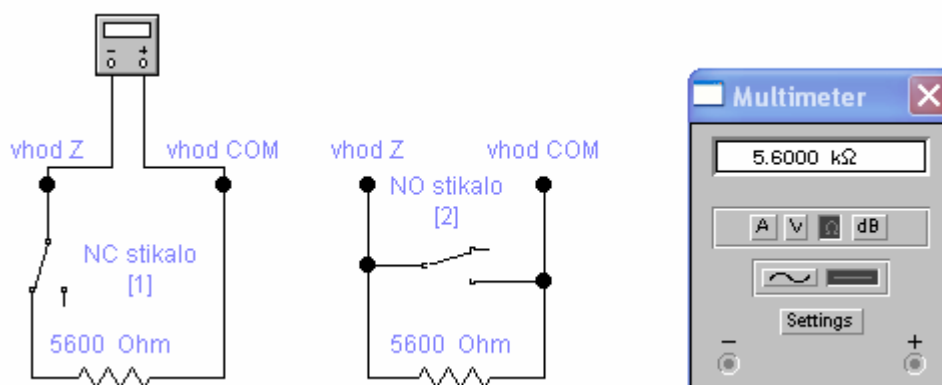
Slika 37: Pregled povezav alarmne centrale in razširitvenih vmesnikov (modulov).

NAPRAVA	KOLIČINA	CENA	CENA SKUPAJ
Alarmna centrala PC1864	1	153 €	153 €
Tipkovnica PK5500	2	138 €	276 €
Razširitveni modul PC5108	4	23 €	92 €
Komunikator GSM/GPRS	1	300 €	300 €
Senzor tipa PIR, LC-100PI	8	20 €	160 €
Senzor tipa PIR&MW, LC-104	6	52 €	312 €
Magnetni kontakt, SM35WH	10	4 €	40 €
Požarni (dimni) senzor S30	6	37 €	222 €
Notranja sirena in bliskavica, MOS1	3	15 €	45 €
Zunanja samonapajalna sirena	1	70 €	70 €
Bariera	2	180 €	360 €
SKUPNA CENA			2030 €

Tabela 14: Popis materiala za omenjen objekt.

8.1.5. Vezava senzorjev priključenih na področja (Zx)

Področja priključimo na priključka COM in na poljubno področje Zx. Področja so lahko zaključena kot normalno odprta (Normally Off - NO) stikala, normalno zaprta (Normally Closed - NC) z enojnim zaključnim uporom (SEOL) in normalno zaprta z dvojnimi zaključnimi uporom (DEOL). Za večjo varnost in zanesljivost sistema je priporočljiva vezava DEOL ali vsaj SEOL. Pri vezavi zaključnih uporov nam centrala meri upornost vezave in nam tako poveča učinkovitost alarmnega sistema. V primeru neuporabe zaključnih uporov, nam lahko vlomilec enostavno prekine kabel ali žice področja stakne v kratek stik. Alarmna centrala ne bo zaznala spremembe in tako bo alarm onesposobljen.

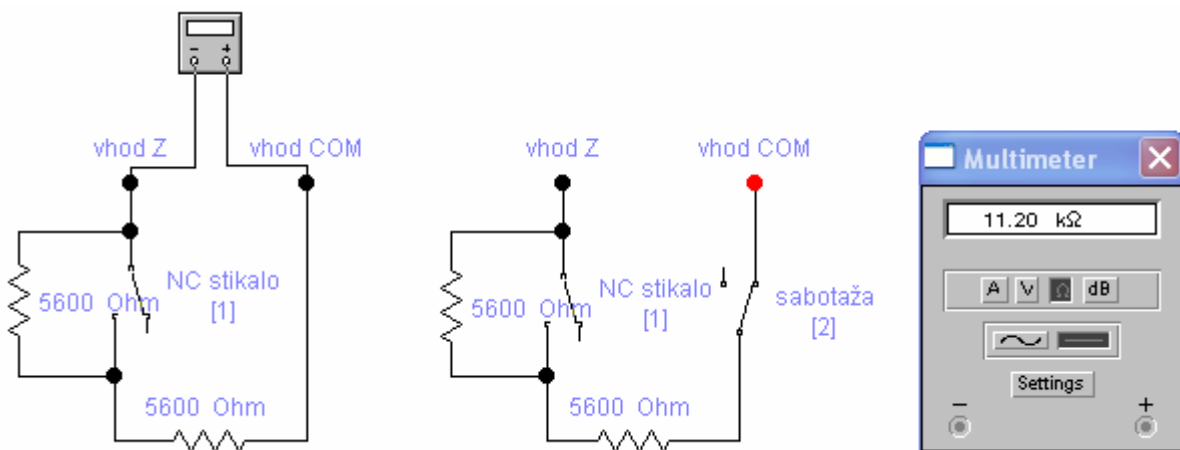


Slika 38: Primer vezave SEOL v z NC stikalom (levo) in NO stikalom (desno).

Pri vezavi senzorjev vedno uporabimo upore vrednosti 5,6 k Ω . Kot vidimo na sliki 38 je upornost zanke 5,6 k Ω , kar pomeni, da je senzor v normalnem stanju. Senzor je ponazorjen z NC stikalom (slika 38, levo) ali z NO stikalom (slika 38, sredina). Katerakoli vrednost, drugačna od upornosti 5,6 k Ω , nam vedno sproži alarm. Če vlomilec hoče narediti kratek stik med Z in COM, je upornost 0 Ω . Alarmna centrala zazna napako in alarm je sprožen. Če prekinemo zanko, dobimo neskončno upornost kar nam tudi sproži alarm. V primeru proženja področja se v prvem primeru (slika 38, levo) stikalo NC izklopi, v drugem pa se stikalo NO

vklopi. V prvem primeru je upornost neskončna, v drugem pa 0Ω . V obeh primerih centrala javi napako in sproži alarm. Pri vezavi SEOL moramo vsa sabotažna stikala senzorjev vezati zaporedno na eno področje centrale.

Pri vezavi dvojnih zaključnih uporov lahko opišemo status področja glede na upornost zanke. Kot smo že napisali centrala v primeru izbranega SEOL ali DEOL varovanja meri upornost med vhodoma Z in COM. Primer varovanja z dvojnimi zaključnimi uporovi je prikazan na sliki 39.



Slika 39: Primer vezave DEOL (levo) in vezave DEOL s sabotažnim stikalom (desno).

Pri vezavi DEOL upornost $5,6 \text{ k}\Omega$ pomeni normalno stanje senzorja. Ko senzor zazna gibanje, se NC stikalo razkane in tako dobimo zaporedno vezavo dveh uporov. Skupna upornost zaporedne vezave se sešteva, zato imamo med priključkoma Z in COM upornost $11,2 \text{ k}\Omega$. Če se pojavi kratek stik med Z in COM, pride do napake in upornosti 0Ω . Prav lahko pride do primera, da vlomilec pride do senzorja, ne da bi ga ta zaznal. Vlomilec bo hotel odpreti senzor, vendar bo zaradi nameščenega sabotažnega stikala (tamper stikalo) prekinil povezavo in s tem sprožil signal za sabotažo. Ker se sabotažno stikalo razkane (slika 39, sredina), je upornosti neskončna.

8.2. Programiranje protivlomnega alarmnega sistema s pomočjo programskega zapisnika-navodil za uporabo

V tem poglavju sem opisal samo nekatere pomembnejše nastavitve, ki jih lahko nastavimo pri alarmni centrali proizvajalca DSC. Kot smo že omenili, je programski zapisnik dokument, v katerega monter vpisuje podatke, ki jih je nastavil za določen protivlomni alarmni sistem. Pred programiranjem sistema je priporočljivo, da v programski zapisnik najprej napišemo želene spremembe, nato pa te spremembe vnesemo v sistem preko tipkovnice.

Za vstop v programiranje sistema najprej pritisnemo zvezdico (*), zatem številko osem in serviserjevo geslo, ki je tovarniško na začetku nastavljeno na 5555. Na kratko lahko vstop v programiranje sistema napišemo kot: »*«8«5555«. Za izhod iz programiranja pritisnemo tipko »#«.

Ko vstopimo v programiranje, se prižge dioda ARMED na tipkovnici. Zatem vnesemo tri mestno številko razdelka, ki ga hočemo sprogramirati. Medtem se dioda ARMED ugasne in se prižge dioda READY, kar pomeni, da je tipkovnica pripravljena na vnos podatkov. Razdelek je trimestno število, ki ga vpišemo, ko vstopimo v programiranje sistema. Vsak razdelek ima na voljo določene funkcije in opcije alarmnega sistema. Pri DSC alarmnih centralah imamo na voljo razdelke od »000« pa do »999«.

8.2.1. Podatki o sistemu

Tukaj napišemo vse splošne podatke uporabnika alarmnega sistema. V primeru okvare sistema je pomemben kontakt serviserja ter serviserjevo geslo. Vpisati moramo vse vgrajene module ter njihovo lokacijo, da v primeru servisa ne pride do nepotrebnega iskanja po celotnem objektu. Enako naredimo tudi za tip in lokacijo tipkovnic.

Na naslednji strani je pripravljen spisek vseh področij, ki jih sistem uporablja. Število vseh možnih področij za alarmno centralo PC1864 je 64. Prvih 8 je namenjenih centrali, ostalih 56 pa razširitvenim modulom. Poleg številke področja vpišemo še:

- ime področja (opis naj bo natančen, npr. PIR kuhinja ali MK otroška soba),
- tip področja (definiramo tip področja),
- lastnosti področja (ko predelamo poglavje 8.2.4, tukaj vnesemo končne podatke),
- serijska številka ESN (za identifikacijo brezžičnih in adresabilnih javljalnikov),
- particije (ko predelamo poglavje 8.2.5, tukaj vnesemo končne podatke).

8.2.2. Programiranje tipkovnic

V tem delu vsem tipkovnicam določimo mesto v alarmnem sistemu ter jim nastavimo funkcijske tipke. To je edini razdelek, ki ga moramo opraviti posebej na vsaki tipkovnici. Ostale nastavitve opravljamo samo na eni tipkovnici, te pa se prenesejo na ostale.

Vsaki tipkovnici moramo dodeliti particijo in naslov. To moramo storiti preden se lotimo nadaljnega programiranja. Tipkovnica lahko deluje kot globalna (»0«) ali ena izmed osmih particij (»1«-»8«). Naslovi tipkovnic morajo biti seveda različni. Ko smo že vstopili v programiranje moramo za dodelitev tipkovnic vpisati razdelek »000«. Pod opcijo »0« izberemo nastavitve za particijo in naslov. Prva številka označuje particijo, druga pa naslov.

V našem primeru sem tipkovnici T1-glavni vhod dodelil številko 11, tipkovnici T3-mansarda pa številko 12. Tako sem uporabil samo eno particijo, vsaka tipkovnica pa mora imeti svoj naslov. Pametna izbira večjih particij bi bila, če bi hotel na drugačen način posebej varovati garažo ali poslovni objekt, ki je vezan na skupno centralo. Če je tipkovnica izbrana kot globalna, je potrebno pred uporabo tipkovnice izbrati particijo. To je uporabno, če imamo več tipkovnic (tudi več različnih particij). Tako lahko z globalno (glavno) tipkovnico dostopamo v vse ostale dele objekta.

Pod razdelkom »00«1» sprogramiramo funkcijsko tipko 1, pod opcijo »00«2» funkcijsko tipko 2 in tako naprej do funkcijske tipke 5. Veljavni vnosi za funkcijske tipke so med »00« in »32«. Vsi veljavni vnosi so zapisani v tabeli 15.

V našem primeru sem pustil tovarniške nastavitve. Funkcijska tipka 1 je nastavljena kot nočno varovanje (»03«). Pod funkcijsko tipko 2 je nastavljen normalen vklop (»04«). Sistem lahko vklopimo tudi z osebnim geslom. Pod funkcijsko tipko 3 je nastavljena indikacija vklopa (»06«). Pod funkcijsko tipko 4 je nastavljeno aktiviranje izhoda #2 (»14«), pod funkcijsko tipko 5 pa hitri izhod (»16«).

VNOS	FUNKCIJA	OPCIJA	FUNKCIJA	OPCIJA	FUNKCIJA
00	nima funkcije	11	programiranje gesel ali »*«5»	22	aktiviraj kamero
01	izbira particije 1	12	dodatne funkcije ali »*«6»	23	preklic izklopa
02	izbira particije 2	13	aktiviranje izhoda #1 ali »*«7»1»	24	aktiviraj skupino izklopov
03	nočno varovanje	14	aktiviranje izhoda #2 ali »*«7»2»	25	za uporabo v prihodnosti
04	Normalenvklop	15	splošna govorna pomoč	26	programiranje časa in datuma
05	vklop brez premika ali »*«9»	16	hitri izhod ali »*«0»	27	izbira particije 3
06	indikacija vstopa ali »*«4»	17	vklop nočnih področij ali »*«1»	28	izbira particije 4
07	testiranje sistema ali »*«6»gl.geslo«4»	18	določena govorna pomoč	29	izbira particije 5
08	izklop področij	19	aktiviranje izhoda #3 ali »*«7»3»	30	izbira particije 6
09	pregled napak	20	za uporabo v prihodnosti	31	izbira particije 7
10	pregled alarmov v spominu	21	aktiviranje izhoda #4 ali »*«7»4»	32	izbira particije 8

Tabela 15: Veljavni vnosi za funkcijske tipke [12].

Če nočemo uporabljati funkcijske tipke, jo nastavimo s številko »00«. Pri izbiri particije (»01«, »02«, »27«, »28«, »29«, »30«, »31« in »32«) mora biti tipkovnica nastavljena kot globalna. Pri vnosu »05« se bo alarm vklopil takoj brez izhodne časovne zakasnitve. Pod vnosom »05« nam bo tipkovnica vedno zapiskala, ko bo določen senzor aktiviran.

Če hočemo izklopiti določena področja, ker ne želimo varovanja v določenem prostoru, pritisnemo »*«1» ali pa funkcijsko tipko, ki je nastavljena kot »08«. S smernimi tipkami se premikamo po področjih in izklopimo zelena področja.

8.2.3. Osnovno programiranje sistema

Pod osnovnim programiranjem sistema nastavljam razdelke od »001« do »030«. Najpomembnejši razdelki so od »001« do »004«, kjer definiramo področja (cone). Na voljo imamo 64 področij, torej se področja razdelijo po 16 na en razdelek. Če imamo v sistemu samo centralo in en razširitveni vmesnik PC5108, nastavimo samo razdelek »001«.

Možne vnose za področja prikazuje tabela 16. Pod zakasnitev1 (01) ponavadi nastavimo senzor pri vhodu v stanovanje. V veliki večini primerov je tipkovnica pri vhodu. Ko je alarm vklopljen, bo senzor sprožil alarm takoj, ko se bo iztekla vhodna časovna zakasnitev. Vhodna zakasnitev je čas, ki ga potrebujemo za vnos uporabniške kode na tipkovnici za izklop alarma, ko vstopimo v stanovanje. Izhodna zakasnitev pa je potreben čas izhoda iz stanovanja, ko vklopimo alarm. Sistemske čase, tako vhodno kot izhodno zakasnitev, definiramo v razdelku »005« »01« za particijo 1. Za particijo 2 v razdelku »005« »2« in tako naprej do particije 8.

Pod opcijo takojšnje (03) se alarm sproži takoj, ko je senzor sprožen. Opcija notranje (04) sledi vhodnemu časovnemu zamiku, če je bilo pred tem sproženo področje zakasnitev1 ali zakasnitev2. Notranje je primerno takrat, če tipkovnice nimamo postavljene pred vhodom, ampak v drugem prostoru. Ko vstopimo v objekt nas vhodni senzor (nastavljen kot zakasnitev1) zazna in začne odšteti čas, ki smo ga definirali v razdelku »005«.

VNOS	FUNKCIJA	VNOS	FUNKCIJA
00	Neuporabljeno področje	20	24-urna zmrzal
01	Zakasnitev1	21	24-urna sklenjena sabotaza
02	Zakasnitev2	22	Kontaktni vklop s ključem
03	Takojšnje	23	Bi-polarni vklop s ključem
04	Notranje	24	Ni uporabljeno
05	Notranje / nočno	25	Notranje / zamik
06	Zakasnitev / nočno	26	24-urna nealarmna cona
07	Zakasnen 24-urni požar	27	Ni uporabljeno
08	Normalen 24-urni požar	28	Ni uporabljeno
09	24-urni nadzor področja	29	Preverjanje požarnega alarma
10	24-urni nadzor s piskom	30	Požarno področje potrditve
11	24-urni vlom	31	Dnevno področje
12	24-urni rop	32	Takojšnje nočno področje
13	24-urni plin	33	Ni uporabljeno
14	24-urna vročina	34	Ni uporabljeno
15	24-urni medic. alarm	35	24-urna sirena / piskač
16	24-urna panika	36	Ni uporabljeno
17	24-urna nujnost	37	Nočno področje
18	24-urni sprinkler	87	Zakasnen 24-urni požar(brezžični)
19	24-urna napaka vode	88	Normalen 24-urni požar(brezžični)

Tabela 16: Možni vnosi področij [12].

Notranje / nočno področje (05) deluje enako kot notranje s to razliko, da je izklopljeno v nočnem varovanju. Zakasnitev / nočno področje (06) deluje enako kot zakasnitev1, vendar je izklopljeno v nočnem varovanju. To opcijo vključimo v primeru, ko ponoči velikokrat

hodimo mimo vhodnih vrat. Alarm se ne bo sprožil, v normalnem vklopu sistema pa bo varoval vhod z vhodno zakasnitvijo.

Pod vnosom zakasnen 24-urni požar (07) bo sirena sprožena takoj (tudi če ni vklopljen alarm), prenos pa bo zakasnen za 30 sekund. Če se pritisne katerikoli tipka, bo prenos zakasnen še za dodatnih 90 sekund. Če ne pritisnemo tipke ali če bo sprožen katerikoli drugi požarni senzor, bo alarm prenesen takoj. Če je bil sprožen lažni alarm, moramo požarni senzor resetirati. Pri vnosu 87 deluje področje enako z razliko, da uporabljamo brezžične senzorje. Pri vnosu normalen 24-urni požar (08) bosta sirena in prenos sprožena takoj (uporaba s požarnimi tipkami), vnos 88 pa se uporablja za isti namen za brezžične senzorje. Pri tistem alarmu (09) se sirena in pisk tipkovnice ne sprožita, alarm pa je prenesen na dežurni center in shranjen v spomin dogodkov. Pri 24-urnem nadzoru s piskom (10) je alarm prenesen na dežurni center, namesto sirene pa se sproži pisk tipkovnice. Pri vnosu od 11-20 bo sprožena sirena in alarm bo takoj prenesen na dežurni center. Razlika je v tem, da so javljeni drugačni dogodki v komunikacijskem formatu.

24-urna sklenjena sabotaza (vnos 21) je namenjena zaščiti vdora v naprave. Če je sproženo to področje, je alarm sprožen takoj, serviser pa mora vstopiti v programiranje alarmnega sistema, preden je ponovno možno vklopiti sistem. Pod vnosom 22 bo kontakt sprožil področje in s tem vklopil ali izklopil alarmni sistem. To področje ne smemo nastaviti kot globalno. Pri vnosu 23 bo stanje tega področja določalo ali bo sistem vklopljen ali izklopljen. Če je področje sproženo, bo sistem vklopljen, če pa je področje v normalnem stanju, bo sistem izklopljen. Pri vnosu 25 (notranji zamik) bo pri normalnem vklopu področje delovalo kot notranje, ob nočnem varovanju pa ima področje vhodni časovni zamik. Vnos 29 nastavi področje za preverjanje požarnih senzorjev. Ko se vklopijo, jih področje izklopi (resetira) za 20 sekund in s tem potrdi, da so senzorji sproženi. Nato se senzorji ponovno vklopijo za 10 sekund. Če pride do ponovnega alarma v roku 60 sekund se takoj sproži alarm. Ko se požarno področje potrditve (30) aktivira, začne tipkovnica piskati in informacija je poslana na dežurni center. Zvok je neprekinjen dokler se ne vpiše uporabniško geslo.

V dnevnem področju (31) imamo različne možnosti. Če je sistem izklopljen, bo aktiviranje področja povzročilo pisk na tipkovnici, ob vklopljenem sistemu pa bo povzročilo alarm. Takojšnje nočno področje (32) je enako kot takojšnje (03) s to razliko, da je izklopljeno v nočnem varovanju (Stay mode). Pri vnosu 35 se bo takoj sprožil alarm. Če bo sistem vklopljen, bo aktiviral sireno/zvočnik (BELL), ob izklopljenem sistemu pa bo vklopljen piskač tipkovnice.

V razdelku »006« lahko serviser nastavi geslo za vstop v programiranje. Kot smo že opisali, nam izhod PGM sklene stikalo na maso ob določenem dogodku. Izhode PGM nastavljamo v razdelkih »009«, »010« in »011«. Možnosti dodatnih izhodov nam prikazuje tabela 17.

Lastnosti opcij izhodov PGM nastavljamo v razdelkih od »501« do »514«. Vsak izhod PGM ima možnost 8 nastavljenih opcij. Razdelek »501« velja za PGM1, »502« za PGM2 in tako do PGM14. Za vnose izhodov PGM 01,03-08, 11-22, 25, 26, 28, 33 in 34 imamo na voljo samo opcijo 3. Če imamo vključeno opcijo 3 (normalen/obrnjen izhod) imamo normalno delujoč

VNOS	FUNKCIJA
01	Sirena vlomnega ali požarnega alarma, <i>izhod bo aktiviran ko bo particija v alarmu</i>
02	Za uporabo v prihodnosti.
03	Resetiranje senzorjev, <i>izhod bo aktiviran za 5 sekund ko pritisnemo ukaz »*«»7«»2 ali ko je zaznana preverjanje požarnega alarma (aktivacija področja 29)</i>
04	Za 2-žilne požarne senzorje, <i>nastavi izhod za vhod (samo PGM2)</i>
05	Stanje sistema/particije, <i>izhod bo aktiven ko bo alarm vklopljen pri vseh particijah</i>
06	Sistem/particija pripravljena na vklop, <i>izhod bo aktiven ko bodo vse particije pripravljene na vklop (ko bo prižgana Ready LED dioda)</i>
07	Sledi pisku tipkovnice, <i>izhod bo aktiven ob pisku tipkovnice</i>
08	Uslužnostni izhod, <i>izhod bo aktiven ob aktivaciji vhodnega/izhodnega čas. Zamika ob vklopljenem sistemu. Izhod bo aktiven še 2 minuti po izklopu sistema</i>
09	Indikacija napake, <i>izhod bo vklopljen ko bo zaznana določena napaka</i>
10	Sklenjen ob določenem alarmu, <i>izhod bo aktiviran ob določenem pogoju na particiji</i>
11	Sabotaža sistema, <i>izhod bo aktiviran ob vsakem pogoju sabotaže</i>
12	Napaka telefona in alarm, <i>izhod bo aktiviran, če bo prekinjena telefonska linija</i>
13	Potrditev komunikacije, <i>izhod bo aktiviran za 2 sekundi, ko bo prejet potrditveni signal "kiss-off" od nadzornega centra</i>
14	Začetni ozemljitveni impulz, <i>izhod se bo aktiviral za 2 sekundi, ko bo centrala posegla v telefonsko linijo</i>
15	Aktiviranje PGM izhoda preko DLS, <i>izhod je lahko aktiviran s pomočjo DLS-ja</i>
16	Za uporabo v prihodnosti
17	Stanje sistema – dnevni režim, <i>vhod je aktiviran ko so vse particije vklopljene v dnevnem režimu (Away mode)</i>
18	Stanje sistema – nočni režim, <i>vhod je aktiviran ko so vse particije vklopljene v nočnem režimu (Stay mode)</i>
19	Ročno aktiviranje izhoda PGM1, <i>izhod se aktivira ko pritisnemo »*«»7«»1«</i>
20	Ročno aktiviranje izhoda PGM2, <i>izhod se aktivira ko pritisnemo »*«»7«»2«</i>
21	Ročno aktiviranje izhoda PGM3, <i>izhod se aktivira ko pritisnemo »*«»7«»3«</i>
22	Ročno aktiviranje izhoda PGM4, <i>izhod se aktivira ko pritisnemo »*«»7«»4«</i>
23	Tihi 24-urni vhod (samo PGM2), <i>PGM2 izhod se spremeni v tihi 24-urni vhod</i>
24	Zvočni 24-urni vhod (samo PGM2) , <i>PGM2 izhod se spremeni v zvočni 24-urni vhod</i>
25	Izhod zakasnjenega požara in vloma, <i>izhod se aktivira šele po iztečenem zak. času</i>
26	Test akumulatorja, <i>izhod se aktivira za 10 sekund ob polnoči, če je akumulator OK</i>
27	Ni definirano
28	Izhod Holdup, <i>izhod se bo aktiviral, ko bo sproženo področje 24-urni rop</i>
29	Sledi področju 1-8, <i>izhod je aktiven če je katerokoli področje aktivno (sproženo)</i>
30	Spomin alarma particije, <i>izhod je aktiven če je vklopljen alarm na izbrani particiji</i>
31	Alternativni komunikator, <i>izhod je aktiven po določenem alarmu</i>
32	Izkop po sproženem alarmu, <i>izhod je aktiven 5 sekund, ko izklopimo aktiviran alarm</i>
33	Stanje sirene in dostop programiranja, <i>izhod je aktiviran, ko je aktiviran BELL, programiranje tipkovnic ali ko je povezava DLS povezana</i>
34	Daljinski vklop brez funkcije bypass, <i>izhod je aktiven ko je vklopljen dnevni ali nočni režim in ko ni nobeno področje izklopljeno (bypass)</i>
35	Sledi področju 9-16, <i>izhod je aktiven če je katerokoli področje aktivno (sproženo)</i>
36	Sledi področju 17-24, <i>izhod je aktiven če je katerokoli področje aktivno (sproženo)</i>
37	Sledi področju 25-32, <i>izhod je aktiven če je katerokoli področje aktivno (sproženo)</i>
38	Sledi področju 33-40, <i>izhod je aktiven če je katerokoli področje aktivno (sproženo)</i>
39	Sledi področju 41-48, <i>izhod je aktiven če je katerokoli področje aktivno (sproženo)</i>
40	Sledi področju 49-56, <i>izhod je aktiven če je katerokoli področje aktivno (sproženo)</i>
41	Sledi področju 57-64, <i>izhod je aktiven če je katerokoli področje aktivno (sproženo)</i>

Tabela 17: Možni vnosi za izhode PGM.

izhod, kar pomeni, da bo izhod aktiviran ob določenem dogodku. Če pa opcija ni izbrana, bo izhod stalno aktiviran in bo ob dogodku neaktiven.

Za vnose 03 in 19-22 imamo poleg opcije 3 na voljo še opcijo 4 (čas delovanja izhoda PGM /ročni izklop) in 5 (geslo/brez gesla). Če imamo vklopljeno opcijo 4, bo izhod aktiviran za določen čas, ki ga nastavimo v razdelku »170«. Če pa opcija ni izbrana, bo izhod aktiviral in deaktiviral uporabnik. Če imamo vklopljeno opcijo 5, pa moramo za aktiviranje izhoda vnesti veljavno geslo (po ukazu »*«»7«»x«).

Izhod PGM pri vnosu 09 (indikacija napake) ima povsem druge nastavitve opcij. Če je določena opcija izklopljena, se izhod ne bo aktiviral. Če pa je vklopljena, imajo opcije naslednje lastnosti:

- Opcija 1) izhod PGM bo aktiviran, če se pojavi napaka "nujen servis" (prazen akumulator, napaka sirene, napaka sistema, sabotaza sistema, nadzor sistema),
- Opcija 2) izhod PGM bo aktiviran, če pride do izpada omrežne napetosti,
- Opcija 3) izhod PGM bo aktiviran, če pride do izpada telefonske linije (TLM),
- Opcija 4) izhod PGM bo aktiviran, če pride do neuspešne komunikacije z dežurnim centrom (FTC),
- Opcija 5) izhod PGM bo aktiviran, če pride do napake na področju (Zone fault),
- Opcija 6) izhod PGM bo aktiviran, če pride do sabotaze področja (Zone tamper),
- Opcija 7) izhod PGM bo aktiviran, če pride do prenizke napetosti ne enem od brezžičnih senzorjev,
- Opcija 8) izhod PGM bo aktiviran, če sistemska ura ni več pravilno nastavljena.

Pri izhodu PGM (vnos 10) imamo naslednjih 8 opcij:

- Opcija 1) izhod PGM bo aktiviran, če se zgodi vlomni alarm (burglary alarm),
- Opcija 2) izhod PGM bo aktiviran, če se zgodi požarni alarm (fire alarm),
- Opcija 3) izhod PGM bo aktiviran, če se pritisne panik tipko (panic alarm),
- Opcija 4) izhod PGM bo aktiviran, če se zgodi zdravniški alarm (medical alarm),
- Opcija 5) izhod PGM bo aktiviran, če se zgodi nadzorni alarm (supervisory alarm),
- Opcija 6) izhod PGM bo aktiviran, če se zgodi prioritetni alarm (priority alarm),
- Opcija 7) izhod PGM bo aktiviran, če se zgodi rop (24-hour hold-up alarm),
- Opcija 8) če je opcija vključena, bo izhod PGM aktiviran za čas delovanja izhoda (razdelek »170«), če pa je opcija izključena, je izhod aktiven dokler ne vtipkamo uporabniško geslo.

Če za izhod PGM izberemo sledenje področju (vnos 29, 35-41), imamo pod opcijo 3 enako možnost normalnega ali obratnega izhoda. Pod opcijo 8 pa imamo na voljo, da izberemo logični ALI (OR) ali logični IN (AND) izhod. Ko izhod PGM sledi logiki AND bo vklopljen, ko bo vseh 8 področij aktiviranih. Nato se bo izklopil, ko bo vsaj eden prišel v normalno stanje. Ko pa izhod PGM sledi logiki OR bo vklopljen, ko bo vsaj eno področje aktivirano. Ko bodo vsa področja v normalnem stanju, se bo izhod PGM izklopil.

V razdelkih od »551« do »564« lahko vsem 14 izhodom PGM določimo kateri particiji bodo dodeljeni. Izhodi so lahko dodeljeni večim particijam.

V razdelku »170« lahko nastavimo čas delovanja izhoda PGM. Veljaven vnos je med 001 in 255 sekund. Če izberemo vnos 11, lahko v razdelku »171« nastavimo čas delovanja izhoda PGM ob sabotaži. Veljaven vnos je med 001 in 255 minut. Za zakasnitev začetka delovanja sirene ob sproženem alarmu lahko v razdelku »171« nastavimo čas zakasnitve.

Pod razdelkom »012« imamo možnost zaklepanja tipkovnice. Za prvi vnos omejimo število nepravilnih vnosov pred zaklepanjem (001-255), za drugi vnos pa vnesemo čas zaklenitve tipkovnice (000-255). Če hočemo funkcijo izklopiti, vnesemo številko 000. Ta funkcija nam lahko pride prav, ko hoče vlomilec uganiti geslo. V razdelku »020« lahko definiramo eno področje, ki ga ima na razpolago tipkovnica.

Od razdelka »013« imamo naprej 10 razdelkov, ki opisujejo sistemske opcije. Pri vsakem razdelku imamo na razpolago 8 opcij za nastavitve. Tovarniške nastavitve so vpisane poleg opcij, sami jih pa lahko vklopimo ali izklopimo.

V našem primeru (slika 34, 35 in 36), sem glavni vhod (S9) in stranski vhod (S8) definiriral kot zakasnitev1. Vhodno zakasnitev sem nastavljal na 30 sekund, izhodno pa na 45 sekund. Senzorje S11, S12, S13 in S14 sem nastavljal kot takojšnje nočno področje zaradi nočnega varovanja v mansardi. Vse ostale senzorjev in magnetne kontakte sem nastavljal kot takojšnje področje. Področje bo ob vklopljenem alarmu takoj sprožilo alarm, ko bo stanje sproženo. Za programabilne izhode PGM1 do PGM4 sem nastavljal vnos 01 (sirena vlomnega in požarnega alarma). Na izhod PGM1, PGM3 in PGM4 sem priklopil vse tri bliskavice (J1, J2 in J3), ki so postavljene vsaka v svoje nadstropje. Na izhod PGM2 pa sem priklopil zunanjo sireno J4 zaradi večje tokovne obremenitve. Pod prvo kodo sistemskih opcij (razdelek »013«) sem vklopil zaključne upore področij (opcija 1) in dvojne zaključne upore (opcija 2) za boljšo varnost pri delovanju in preprečitvi sabotaže senzorjev. V tretji kodi sistemskih opcij (razdelek »015«) smo vklopili TLM. Nadzor telefonske linije bo v tem primeru deloval in centrala bo v primeru izpada javila napako. Vse ostale sistemske opcije za delovanje ni potrebno spreminjati.

8.2.4. Podrobnejše programiranje sistema

V tem poglavju lahko podrobneje definiramo sistem. Za vsako področje (cono) lahko nastavimo 12 lastnosti in tako do potankosti definiramo način delovanja. Na izbiro imamo naslednje opcije, ki so podane v tabeli 18.

Za vklop preverjanja vloma "Cross zone" načina moramo v razdelku »018« vklopiti opcijo 6. Ta možnost potrebuje večkratno aktiviranje alarma. Ko se področje aktivira, se sproži odštevanje in izhod PGM (če je nastavljen). Če v času odštevanja ni ponovnih sproženj se zabeleži dogodek "nepreverjen alarm" in centrala se vrne v normalno stanje. Če pa je v času odštevanja področje ponovno sproženo, se aktivira alarm.

Področja za 8-področno centralo definiramo v razdelkih od »101« do »108«, za razširitvene vmesnike pa od razdelka »109« do »164«.

V razdelku »165« lahko nastavimo največje število poskusov prenosov na telefonsko številko, preden centrala javi napako neuspešne komunikacije z dežurnim centrom (FTC). Tretjo telefonsko številko lahko uporabimo kot rezervo za prvo telefonsko številko (razdelek »380«)»5«.

OPCIJA	FUNKCIJA
»1« Slišno/tiho	ON: aktivno področje sproži sireno
	OFF: aktivno področje sproži tihi alarm
»2« Konstantno/pulzno	ON: sirena se proži konstantno (protivlomni alarmni sistem)
	OFF: sirena se proži pulzno (javljanje požara)
»3« Indikacija DA/NE	ON: indikacija vstopa deluje (chime)
	OFF: indikacija vstopa ne deluje
»4« Izklop DA/NE	ON: področje je možno ročno izklopiti (bypass) z ukazom »*«)»1«
	OFF: področje ni možno izklopiti
»5« Prisila DA/NE	ON: particijo je možno vklopiti tudi, če je področje aktivirano
	OFF: področje ne sme biti aktivirano za vklop alarma
»6« Števec DA/NE	ON: sistem prekine pošiljanje dogodkov po določenem številu alarmov
	OFF: centrala bo vedno poslala dogodek v primeru alarma
»7« Zakasnitev DA/NE	ON: centrala zakasni prenos na dežurni center
	OFF: centrala takoj sproži prenos na dežurni center
»8« Brezžično DA/NE	ON: področje je brezžično ali z adresabilno tehniko
	OFF: področje je žično (področje na alarmni centrali, razširitvenem vmesniku ali področje na tipkovnici)
»9« Cross zone DA/NE	ON: področje ima vključeno funkcijo "Cross zone"
	OFF: področje deluje normalno
»10«-»13«	Za uporabo v prihodnosti
»14« NC zanka	ON: področje je definirano kot normalno zaprto (NC zanka)
	OFF: področje bo sledilo EOL nastavitvi v razdelku »013«
»15« SEOL vezava	ON: področje je definirano kot SEOL zanka
	OFF: področje bo sledilo EOL nastavitvi v razdelku »013«
»16« DEOL vezava	ON: področje je definirano kot DEOL zanka
	OFF: področje bo sledilo EOL nastavitvi v razdelku »013«

Tabela 18: Opis 12 lastnosti, ki jih lahko definiramo za vsako področje.

V razdelku »168« in »169« lahko nastavimo premik ure za eno ali dve ure naprej ali nazaj. Tako nam ni treba skrbeti za poletni in zimski čas. V razdelkih od »181« do »188«, lahko za vsako particijo posebej vklopimo urnik avtomatičnih vklopov z vnosom štirimestne številke v formatu (ura:minuta) za vsak dan posebej. Tovarniško so vsi vklopi onemogočeni (0000). Če se vklop alarma ne more izvesti, lahko v razdelku »175« nastavimo zakasnitev avtomatičnega vklopa v minutah. Veljavni vnosi minut so med 000 in 255. V razdelkih od »190« do »199« pa lahko definiramo opozorilni čas pred vklopom sistema.

V našem primeru smo popravili senzor S9 tako, da smo vključili opcijo prisila (opcija 5). Senzor S9 pokriva tipkovnico T2. Ob vklopu sistema morajo biti vsi senzori v normalnem (nesproženem) stanju. Ko smo vključili to opcijo, lahko vklopimo varovanje kljub našemu premikanju. Ker smo v razdelku »013« nastavili vezavo DEOL, moramo za vse magnetne

kontakte in požarne senzorje vklopiti NC zanko (opcija 14), ter tako izklopiti varovanje z dvema zaključnima uporoma. Zaradi zahteve uporabnika smo pri vseh javljalnikih izklopili indikacijo vstopa (opcija 3), saj smo bili mnenja, da je pisk tipkovnice ob zaznavanju senzorjev moteč.

8.2.5. Programiranje področij in particij

Kot smo že opisali je področje definirano kot javljalnik, ki pokriva določeno področje (cono). Na alarmni centrali jih priključimo na priključka Z1 in COM (glej sliko 20). Particija pa je popolnoma ločen podsistem, ki deluje neodvisno od drugega. Na alarmni centrali PC1864 lahko ustvarimo do 8 particij, na PC1832 4 particije in samo 2 particiji na PC1616. Če hočemo nastaviti sistem na več particij, moramo vsako posamezno particijo vključiti v razdelku »201«. Particija 1 je vedno vključena in jo ne moremo izključiti, saj sistem ne bi deloval. Vse ostale particije lahko vključimo, tovarniško pa so vse izključene. Na katerokoli particijo lahko dodelimo katerokoli področje. Področja, ki so dodeljena večim particijam, so globalna področja. Ta področja bodo vključena samo, kadar bodo vključene vse particije. Izključena pa bodo takrat, ko bo izključena vsaj ena particija. Tovarniško so področja od 1 do 8 (alarmna centrala) dodeljena particiji 1.

Če uporabljamo dodatna področja ali ko aplikacija zahteva več kot eno particijo, moramo razdeliti področja določenim particijam. To naredimo v razdelkih od »202« do »265«. Za particijo 1 dodeljujemo področja od 1 do 64 v razdelkih od »202« do »209«. Vsak razdelek ima 8 področij. Za particijo 2 dodeljujemo področja od 1 do 64 v razdelkih od »210« do »217 in tako naprej do osme particije.

Področja, ki so sprogramirana kot 00 (izklopljena), moramo odstraniti iz vseh particij. Gesla lahko dodeljujemo za vsako particijo posebej. Tipkovnice lahko, kot smo že napisali v poglavju 8.1, dodelimo posameznim particijam ali vsem particijam (globalno delovanje). Vsako particijo lahko sprogramiramo, da sporoča drugačno razpoznavno geslo. Nekatere od programibilnih izhodnih opcij se lahko prav tako določijo posameznim particijam.

V našem primeru imamo samo eno particijo. V razdelku »202« označimo vseh osem področij, saj so to področja alarmne centrale. Razširitveni modul RM1 pokriva razdelek »203«, RM2 razdelek »204«, RM3 razdelek »204« in RM4 razdelek »205«.

8.2.6. Programiranje komunikatorja alarmne centrale

Komunikator alarmne centrale nastavljamo v razdelkih od »301« do »382«. Najpomembnejša nastavitve v tem poglavju je vključitev komunikatorja v razdelku »380« »1«. V razdelkih »301«, »302« in »303« nastavimo 3 telefonske številke, ki jih bo alarmna centrala poklicala v primeru alarma. Pri vpisu telefonske številke mora biti prvi znak vedno D, ki pomeni, da išče znak proste linije. Na koncu telefonske številke vnesemo številko F za konec telefonske številke. Če uporabljamo tretjo telefonsko številko jo moramo najprej omogočiti (razdelek »380« »5«). Tretja telefonska številka je lahko rezerva za prvo telefonsko številko, lahko pa centrala tudi izmenično kliče prvo in tretjo telefonsko številko (razdelek »380« »6«).

V razdelku »350« moramo vpisati številko komunikacijskega formata, ki ga bodo uporabljale telefonske številke. Prenosi na tretjo telefonsko številko se opravljajo v istem formatu kot ga nastavimo na prvi telefonski številki. Možni komunikacijski formati so podani v tabeli 19.

VNOS	KOMUNIKACIJSKI FORMAT
01	Handshaking (usklajevalni način) 20 bitov/s, 1400Hz
02	Handshaking (usklajevalni način) 20 bitov/s, 2300Hz
03	DTMF Contact ID
04	SIA FSK
05	Pager
06	Rezidenčni klic
07	Handshaking (usklajevalni način) 10 bitov/s, 1400Hz
08	Handshaking (usklajevalni način) 10 bitov/s, 2300Hz
09	Privatna linija-javljanje številke sproženega področja
10	Scantronics
11	Za uporabo v prihodnje
12	Robofon
13	CESA 200

Tabela 19: Komunikacijski formati za prenos alarma.

V našem primeru smo uporabili klic privatne linije-rezidenčni klic (06) ali klic privatne linije-javljanje številke sproženega področja (09). Če bi v našem sistemu varovali hišo s pomočjo VNC-ja, bi uporabili komunikacijski format DTMF Contact ID. Ko se sproži alarm, uslužbenci v VNC natančno vedo, kje (na kateri particiji in področju) in kakšen tipa alarma se je zgodil. Tako alarmna centrala, kot komunikator GSM podpirata ta komunikacijski format.

Pri rezidenčnem klicu alarmna centrala, v primeru alarma po telefonski liniji pokliče nastavljene telefonske številke. Nato centrala odda ID ton in čaka na odgovor (handshake). Za potrditev alarma pritisnemo tipko 3, 6 ali 9 na telefonu s tonskim izbiranjem in jo držimo 2 sekundi. Ko centrala sprejme ton, začne z 20-sekundnim prenosom alarmnega tona. Če v istem času pride do več alarmov, bo prenesen samo prvi alarm. V razdelku »166« nastavimo čas čakanja centrale na naš odgovor ali odgovor dežurnega centra. Če ga centrala v tem času ne sprejme, bo klic neveljaven. Linija se bo prekinila, klic pa bo ponovljen. Tovarniško je čas čakanja nastavljen na 40 sekund. V razdelku »165« pa nastavimo največje število klicev na telefonsko številko preden centrala javi napako neuspešne komunikacije (FTC).

Pri privatni liniji je postopek podoben rezidenčnemu klicu s to razliko, da nam javi številko sproženega področja. V primeru alarma nam centrala po telefonski liniji pokliče nastavljene telefonske številke. Centrala nato oddaja dvojni pisk vsake 3 sekunde. To je sporočilo uporabniku, da ga kliče alarmna centrala. Uporabnik s pritisnjeno tipko sprejme klic enako kot pri rezidenčnem klicu. Nato bo centrala s piski določila, katero področje je aktivirano (npr. če centrala pošlje 3 piske pomeni, da je področje 3 v alarmu). Uporabnik spet s tipko pove centrali, da je sprejel signal. Če je sproženo še eno področje, bo centrala ponovila postopek in uporabniku s piski določila, katero področje je aktivirano.

8.2.7. Programiranje izpisov na tipkovnici

Za vstop v programiranje tipkovnic pritisnemo »*«8»«serviserjevo geslo»*«, torej ko smo v načinu programiranja, pritisnemo zvezdico. Če je v sistemu več kot ena tipkovnica LCD, se lahko poimenovanja področij prenesejo tudi na druge tipkovnice. Za prenos izpisov na vse tipkovnice moramo najprej popolnoma sprogramirati eno LCD tipkovnico (samo PK5500 in RFK5500). Nato preverimo ali so vse tipkovnice priključene na KEYBUS povezavo. Nato na sprogramirani tipkovnici vstopimo v način programiranja tipkovnice in vpišemo razdelek »998«. Ko se prenos na ostale tipkovnice konča, pritisnemo »#« za izhod.

Imena področij in druge izpise lahko spremenimo glede na elemente alarmnega sistema in s tem olajšamo uporabo alarmnega sistema lastniku. V razdelkih od »001« do »064« lahko poimenujemo področja (na voljo je 14 znakov). V ostalih razdelkih, ki si sledijo, pa lahko poimenujemo tudi izpis požarnega alarma, izpis neuspešnega vklopa sistema in sporočilo ko izklopimo sprožen alarm. Od razdelka »101« do »108« vpisujemo nazive particij, od razdelka »120« do »151« pa nazive izhodov PGM za vse particije. Za posamezna področja lahko tudi spreminjamo tip zvoka tipkovnice. Izbira ja možna med štirimi različnimi toni.

9. Zaključek

Vsekakor se za vgradnjo tako kompleksnega sistema za protivlomno varovanje ne odloča veliko ljudi. Zdi se jim nepotrebno, saj se ne počutijo ogrožene v kraju kjer živijo. Drugi vzrok je tudi dodaten strošek pri novogradnji objektov, ki bi bil poleg drugih za nekatere prevelik zalogaj. Če pa bi spraševali posameznike, ki so si vgradili sistem protivlomnega varovanja, bi verjetno dobili pozitivne izkušnje. Na to vsekakor vpliva dejstvo, da se počutijo varnejše v svojem stanovanju. Za nekatere objekte kot so banke, muzeji, pošte, itn., ki so bolj zanimivi vlomilcem, pa je sistem protivlomnega varovanja nujen.

V tej nalogi sem predstavil sistem protivlomnega varovanja v hiši. Če bi imeli na voljo kakšen večji objekt ali kakšen poslovni objekt, bi lahko poleg sistema protivlomnega varovanja vgradili tudi kakšen drug sistem. Pri podjetjih je včasih pomembno, kdo je vstopil v nek prostor ob določenem času. V tem primeru bi uporabili sistem pristopne kontrole in registracije delovnega časa. Osnovni elementi sistema pristopne kontrole so: čitalci in kartice, glavna kontrolna enota, ključavnice, programska oprema in registracija delovnega časa.

V spodnjih dveh nadstropjih smo dodali po en protipožarni senzor. V mansardi pa smo zaradi večje požarne nevarnosti dodali požarni senzor v vsak prostor. Glavne naloge protipožarnega sistema so: zgodnje odkrivanje požara, preprečevanje škode, delovanje v najtežjih pogojih, javljanje različnih vrst požara, 24-urno delovanje in zadostitev zakonskim predpisom. Protipožarni sistem mora za učinkovito delovanje odkriti naslednje pojave: nevidni produkti izgorevanja, dim, plamen in toploto. S pomočjo avtomatskih in ročnih (tipka) javljalnikov tako poskrbimo za zanesljivo odkrivanje različnih vrst požarov v različnih okoljih.

Naj kot zadnje omenim sistem video nadzora. Ta je na področju tehničnega varovanja eden novejših in hkrati najhitreje razvijajočih se varnostnih sistemov. V začetku so bili video nadzorni sistemi samo analogni, sedaj pa se večinoma uporablja kombinacija z digitalnimi. Sistem video nadzora sestavljajo naslednji elementi: video kamera, objektiv, monitor, sistem za zaznavanje gibanja, snemalna naprava in enota za shranjevanje podatkov.

Bolj poglobljena raziskava vseh ostalih naštetih sistemov za varovanje bi bila zanimiva nadgraditev moje diplomske naloge. Zanimivo bi bilo tudi medsebojno delovanje sistemov ter prednosti in slabosti le teh.

10. Viri

- [1] Varovanje pred dopustom. Dostopno na:
http://www.varnost.si/varovanje_pred_dopustom
- [2] Dušan Fefer, Avtomatski sistemi za odkrivanje in javljanje požarov in prenos alarmnih sporočil. Dostopno na:
http://www.sos112.si/slo/tdocs/apz_fefer.pdf
- [3] Gorenje d.d., Protivlomni sistemi. Dostopno na:
<http://www.gorenjevarovanje.si/a1.htm>
- [4] Fortuna d.o.o., Protivlomni sistemi. Dostopno na:
http://www.fortuna.si/pdf/protivlomni_sistemi.pdf
- [5] Overview of EN50131. Dostopno na:
<http://www.crosbyintruder.co.uk/en50131-overview>,
- [6] Koncern Sintal, Sintalček, 39.številk, marec 2008. Dostopno na:
www.sintal.si/info/sintalcek/Sintalcek%2039.pdf
- [7] Mobicom d.o.o., Alarmne centrale. Dostopno na :
<http://www.mobicom.si/default-30002.html>
- [8] Mobicom d.o.o., Zasnova protivlomnega sistema. Dostopno na:
<http://www.mobicom.si/default-22000.html>
- [9] Zveza potrošnikov Slovenije, Elektromagnetno sevanje. Dostopno na:
<http://www.zps.si/okolje/okolje/elektromagnetno-sevanje.html?Itemid=322>
- [10] Rittal d.o.o., Stopnje zaščite IP po EN 60529/IEC 529. Dostopno na:
http://www.rittal.si/services_support/technical_information/IP_zascita.shtml
- [11] DSC Slovenija, DSC katalog 2006. Dostopno na:
http://www.mobicom.si/P/PDF/DSC_Katalog2006.pdf in
DSC Slovenija, DSC katalog 2010. Dostopno na:
http://www.mobicom.si/P/PDF/0-dsc%20katalog_2009.pdf
- [12] DSC, PowerSeries PC1616/PC1832/PC1864 version 4.2 EU Installation Guide, 2008
- [13] Philips Semiconductor, The I²C bus specification, version 2.1, 2000. Dostopno na:
<http://www.nxp.com/documents/other/39340011.pdf>
- [14] SIA Standards, Digital Communication Standard - Ademco ® Contact ID Protocol - for Alarm System Communications. Dostopno na:
www.palmettosecurity.org/index.php/download_file/view/23/
- [15] DSC, GS3055-I GSM/GPRS Alarm Communicator
- [16] Cev RBT in RFS. Dostopno na:
http://www.internetnatrgovina.com/product_info.php?products_id=3228
- [17] Interactive Technologies, ITI Indoor and Outdoor PIR Motion Sensors, 1998. Dostopno na:
<http://www.worthingtondistribution.com/solutions/Manuals/GE%20Interlogix/SAW%20Motion%20Sensors%20Specs.pdf>