SUVREMENI SUSTAVI TEHNIČKE ZAŠTITE I SIGURNOSNI SUSTAVI VOZILA

Kanjer, Davor

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Davor Kanjer

SUVREMENI SUSTAVI TEHNIČKE ZAŠTITE I SIGURNOSNI SUSTAVI VOZILA

ZAVRŠNI RAD

Karlovac, 2019.

Karlovac University of Applied Sciences
Safety and Protection Department

Professional graduate study of Safety and Protection

Davor Kanjer

MODERN TEHNICAL PROTECTION SYSTEM AND SAFETY SYSTEMS OF VEHICLES

FINAL WORK

Karlovac, 2019.

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Davor Kanjer

SUVREMENI SUSTAVI TEHNIČKE ZAŠTITE I SIGURNOSNI SUSTAVI VOZILA

ZAVRŠNI RAD

Mentor:
Marijan Brozović, dipl.ing., v.p.

Karlovac, 2019.

VELEUČILIŠTE U KARLOVCU
KARLOVAC UNIVERSITY OF APPLIED SCIENCES
Trg J.J.Strossmayera 9
HR-47000, Karlovac, Croatia
Tel. +385 - (0)47 - 843 - 510
Fax. +385 - (0)47 - 843 – 579

HRN EN ISO 9001:2009

VELEUČILIŠTE U KARLOVCU

Stručni / **specijalistički studij:** Specijalistički diplomski stručni studij Sigurnosti I zaštite

Usmjerenje:Sigurnost I zaštita na radu Karlovac: 11.12.2018.

ZADATAK ZAVRŠNOG RADA

Student: Davor Kanjer Matični broj:0420416023

Naslov: **SUVREMENI SUSTAVI TEHNIČKE ZAŠTITE I SIGURNOSNI SUSTAVI VOZILA**

Opis zadatka:

- Opisati suvremeni sustav tehničke zaštite
- Opisati sigurnosne sustave na vozilu
- Dati pregled elektroničkih sustava u vozilima
- Dati pregled najznačajnijih sigurnosnih sustava u vozilima

Zadatak izraditi i opremiti sukladno Pravilniku o Završnom ispitu VUK-a.

Zadatak zadan:	Rok predaje rada:	Predviđeni datum obrane:
11.12.2018.	15.04.2019.	29.04.2019.

Mentor: Predsjednik Ispitnog povjerenstva:

Marijan Brozović dipl.ing.,v.pred.

II. PREDGOVOR

U ovom radu pod gornjim naslovom potrebno je navesti i analizirati postojeće sustave tehničke zaštite koji se u suvremenom društvu primjenjuju radi povećanja ukupne sigurnosti i smanjenja ugroženosti.

U tom je smislu potrebno objasniti proces procjene stupnja opasnosti u pojedinim elementima društvene strukture, način funkcioniranja pojedinih sredstava, prednosti i manjkavosti, mogućnost aplikacije te ukazati na potencijalne oblike sustava zaštite koji će se primjenjivati u budućnosti.

III. SAŽETAK

Sigurnost je jedno od rijetkih stanja kojem teže sva živa bića. Sigurnost je normalno stanje živog bića, ali je ono, preko napada na samo biće, stalno na udaru različitih ugroženosti i opasnosti, koje dolaze sa svih strana: iz svemira, s planeta na kojem žive, iz vlastite sredine, od drugih živih bića, pa i iz samog živog bića. Zato se cijeli život provodi u stalnoj borbi s ugroženostima i opasnostima, u nastojanju da se postigne i održi određeni stupanj sigurnosti . **Suvremeno društvo je društvo rizika.**

Rizici i opasnosti postoje u našoj svakodnevnoj socijalnoj okolici, više ili manje su raspoređeni, najčešće neovisno o našoj volji .

Svakog dana svjedoci smo da je život u suvremenom društvu satkan od niza rizika kao što su: terorizam, tehnološki rizici, kriminal i da je život sve opasniji i rizičniji.

KLJUČNE RIJEČI:

- tehnička zaštita
- rizik
- procjena ugroženosti
- perimetar
- sigurnost

III. SUMMARY

Safety is a rare condition to which all the living beings are striving. Safety is a normal state of a living being, ranging from attack on the living being itself, vulnerability to myriad threats and dangers coming from all directions, from the planet they are living on, from their own environment, from other living beings and from within the being itself. Therefore the entire life is being spent in constant struggle with threats and dangers trying to achieve and maintain certain level of safety . Modern society is a risk society.

Risks and dangers in our daily social environment, more or less are arranged, usually without our will .

Every day we realize that life in a modern society is made of risks such as terrorism, technological risks, crime, and that life is becoming filled with more dangerous and risks.

KEY WORDS:

- technical protection
- risk
- threat estimation
- perimeter
- safety

SADRŽAJ

1.UVOD

Pod pojmom tehničke zaštite prema Pravilniku o uvjetima i načinu provedbe tehničke zaštite (N.N., broj 198/03), **tehnička zaštita predstavlja skup radnji kojima se neposredno ili posredno zaštićuju ljudi i njihova imovina, a provodi se tehničkim sredstvima i napravama te sustavima tehničke zaštite kojima je osnovna namjena sprječavanje protupravnih radnji usmjerenih prema štićenim osobama ili imovini[*].**

Mjerama tehničke zaštite mora se postići ispunjavanje šest osnovnih funkcija:

1. Odvraćanje.
2. Usporavanje.
3. Detekcija.
4. Uzbunjivanje.
5. Identifikacija.
6. Odgovor.

Odvraćanje potencijalnog počinitelja kaznenog djela.

Usporavanje neovlaštenog pokušaja prodora ili prodora u štićeno područje postiže se mehaničkim zaprekama: trezorom, sefovima, ogradama i sl.

Detekcija neovlaštenog pokušaja prodora ili prodora ostvaruje se upotrebom tehničkih sredstava za detekciju prisustva neovlaštene osobe.

Uzbunjivanje i identifikacija postiže se sustavom za prijenos i nadzor kojima se prenosi, identificira i objavljuje alarmna situacija na određenom mjestu štićenog objekta/prostora.

Odgovor na alarmnu situaciju vrši tjelesna zaštita, odnosno stražarska služba ili interventna postrojba.

Konceptom tehničke zaštite mora se ostvariti ispunjenje sljedećih funkcija:

ODVRAĆANJE - USPORAVANJE - DETEKCIJA - UZBUNJIVANJE - IDENTIFIKACIJA - ODGOVOR

[*] Pravilnik o uvjetima i načinima provedbe tehničke zaštite (NN broj 198/03).

2. ZONE DETEKCIJE

Da bi se koncepcijom tehničke zaštite postiglo optimalno rješenje, potrebno je tehničku zaštitu podijeliti na zone detekcije (neki autori to zovu “zamišljeni koncentrični krugovi zaštite”). Prema njima za optimalno štićenje nekog objekta potrebno je predvidjeti maksimalno pet (5) zona detekcije, odnosno manje (optimalno 3) ukoliko su takvi uvjeti na objektu.

Zone detekcije:

1. Zona detekcije – detekcija prodora u perimetar.
2. Zona detekcije – detekcija kretanja po perimetru.
3. Zona detekcije – detekcija prodora u objekt.
4. Zona detekcije – detekcija kretanja po objektu.
5. Zona detekcije – detekcija pristupa štićenom sadržaju.

Prva zona je zona detekcije prodora u perimetar i obično se nalazi na ogradi perimetra, a čine je uređaji i sklopovi koji detektiraju pokušaj penjanja preko ograde, podvlačenja pod ogradu i sječenje ograde.

Druga zona detekcije se obično nalazi između ograde ili granice posjeda i imovine ili objekta koji se štiti. Čine je uređaji i sklopovi koji detektiraju bilo kakvo protrčavanje, hodanje ili puzanje kroz zonu.

Treća zona je vanjski prostor objekta ili sobe štićene imovine. Koriste se uređaji i sklopovi kojima se detektira pokušaj prodora u objekt ili sobu.

Četvrta zona je unutrašnjost objekta ili sobe. Za njenu zaštitu se koriste uređaji i sklopovi kojima se detektira kretanje po unutrašnjosti objekta ili sobe.

Peta zona je zona zaštite “osobito važnih sadržaja”. Detektira se svaki pokušaj pristupa ili uklanjanja predmeta zaštite ili pokušaj prodora u zaštitni kontejner.

Promatrajući ovih pet zona kroz prizmu vremena koje se osigurava za intervenciju osoblja zaštite (stražara) evidentno je da najdulji vremenski razmak osigurava prva zona, odnosno treća (ukoliko prve dvije nisu postavljene). Najmanje vremena se osigurava petom zonom i ukoliko ona ne predstavlja dobro zaštićeni sef ili trezor ili je osoblje stražarske službe u neposrednoj blizini, poželjno je kombinirati je sa drugim zonama.

2.1. Koncepcijsko rješenje zadanih mjera tehničke zaštite

Od sustava tehničke zaštite očekuje se da riješi mjere:

- odvraćanja
- usporavanja
- detekciju
- uzbunjivanje i identifikaciju.

Odvraćanje potencijalnog počinitelja kaznenog djela postiže se ugradnjom i primjenom suvremenih sustava tehničke zaštite.

Usporavanje neovlaštenog prodora postiže se postavljanjem različitih mehaničkih barijera ili dogradnjom postojećih prepreka mehaničkim i elektromehaničkim sustavima blokiranja. Rješenje treba odabrati u skladu s operativnim prolazom na kojem se primjenjuje.

Detekcija, uzbunjivanje i identifikacija riješit će se primjenom odgovarajućih sustava tehničke zaštite.

Iz analize je vidljivo da se za isti prostor ili komunikacijsku prometnicu traži ispunjenje mjera odvračanja, usporavanja, detekcije, uzbunjivanja i identifikacije, što nas upućuje na primjenu takvog sustava koji će moći zadovoljiti svih pet ili najmanje dva zahtjeva istovremeno jednim uređajem ili sklopom u zadanom prostoru.

U skladu s:

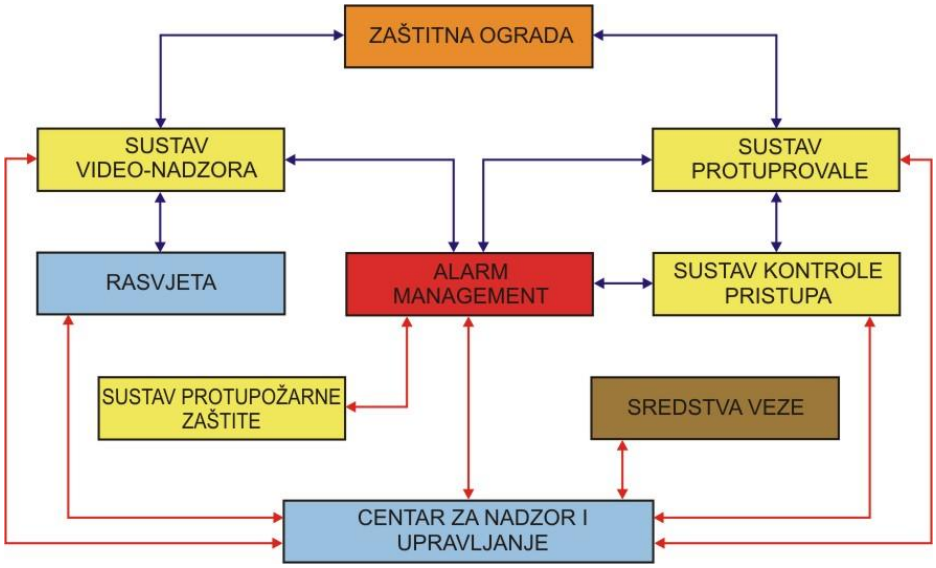
- zahtijevanim mjerama tehničke zaštite pojedinih objekata i perimetara
- procjenom ugroženosti
- današnjim dostignućima na području tehničke zaštite
- ekonomskom opravdanošću uvođenja određenih tehničkih rješenja.

Predlaže se uvođenje određenog sustava tehničke zaštite objekta kao što su: sustav kontrole pristupa, video-nadzora, protuprovale itd.

Sustavi međusobno razmjenjuju informacije preko centralne opreme za obradu signala u nadzornom centru. **Blok shema koncepcije tehničke zaštite**, integralno rješenje prikazano je na **shemi 1.**

Iz blok sheme je razvidna potreba za upravljanjem i nadzorom nad drugim sustavima u svrhu osiguranja odgovarajuće razine sigurnosti, kao i upotreba sustava tehničke zaštite u druge svrhe (protupožarna zaštita).

Osim novih sustava tehničke zaštite, integralno rješenje mora moći prihvatiti i već postojeće sustave, npr. kontrole pristupa i protuprovale, videoportafonsku komunikaciju itd.



Shema 1. Blok shema koncepcije tehničke zaštite

2.2. Temeljne postavke za izbor sustava tehničke zaštite

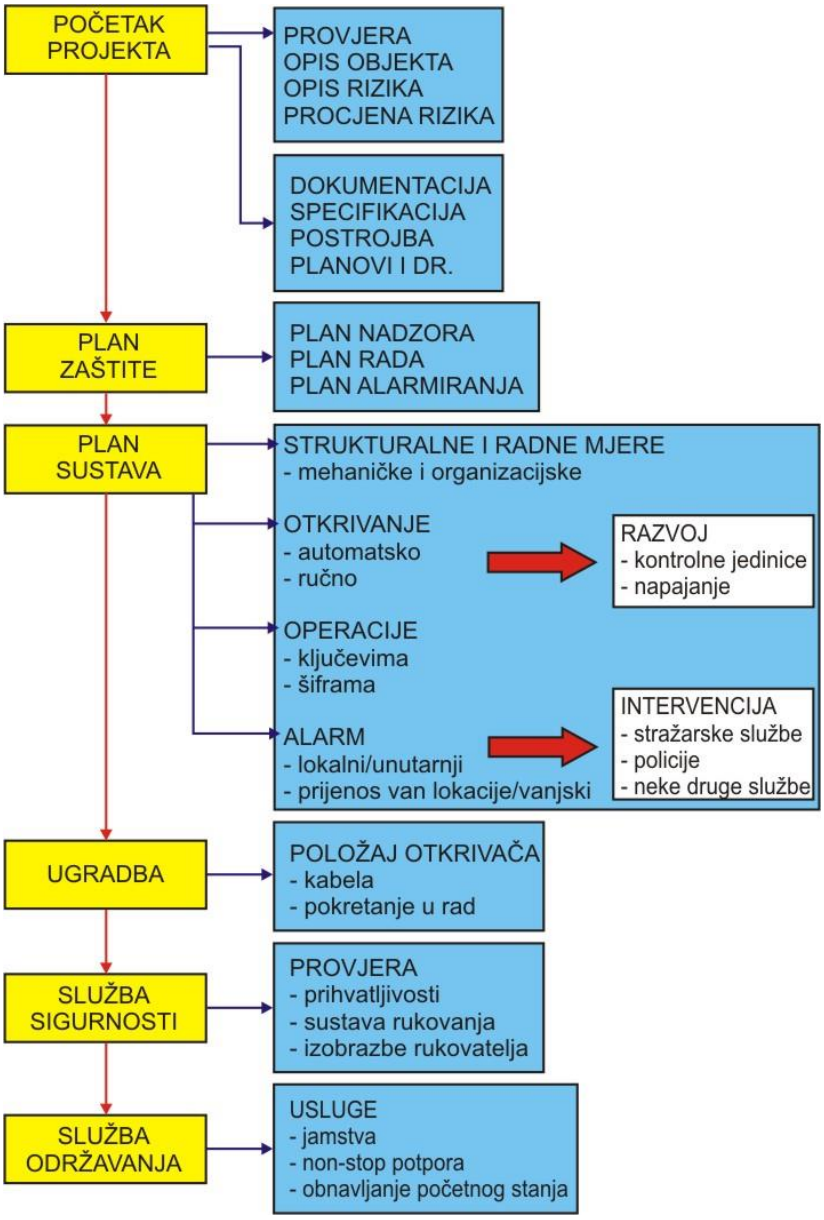
Pri izradi idejnog rješenja tehničke zaštite projektant će se pridržavati sljedećeg:

1. Pravilnika o uvjetima i načinu provedbe tehničke zaštite (N.N. broj 198/03).
2. Koncepcija tehničke zaštite.
3. Iskustvenih spoznaja:
   - izbjegavati sustave koji se sastoje od diskretnih uređaja ili komponenti podložnih čestim kvarovima
   - izbjegavati sustave koji se montiraju izravno na ogradu perimetra zbog podložnosti pobudama alarma zbog slučajnih i nezlonamjernih aktivnosti uz ogradu
   - izbjegavati sustave koji pretjerano ovise o čišćenju perimetra od zelenila i trave
   - izbjegavati sustave koji ovise o metereološkim uvjetima (magla, kiša, snijeg, vjetar)
   - izbjegavati sustave koji rade na načelu detekcije vibracija zbog blizine željezničkog i cestovnog prometa, te strojeva koji proizvode jake vibracije što može prouzrokovati lažne alarme.

4. Zahtjevi proizašli iz specifičnosti lokacije i objekta:
   - zbog velikog broja elektroenergetskih objekata i postrojenja, te mogućih jakih elektromagnetskih smetnji, pri prijenosu signala koristiti optičke kablove
   - pri definiranju opreme i zahtjeva na opremu osobitu pozornost voditi o eksplozivnim zonama
   - izbjegavati sustave koji usporavaju ili ometaju normalne radne procese u objektima.

5. Preporuke EN normi.
6. Preporuke ISO normi.
7. Preporuke IEC normi.
8. Preporuka Udruge tehničke zaštite pri Hrvatskom cehu zaštitara.

Prilikom izbora sustava tehničke zaštite voditi računa da su primjenjena priznata pravila u provedbi tehničke zaštite osoba i imovine, da je njihov razvoj (projektiranje), ugrađivanje, primjena i održavanje (vidi shemu 2.) sukladno projektnoj dokumentaciji, izvedbenoj dokumentaciji i zakonskim odredbama kojima su propisani uvjeti i način provedbe tehničke zaštite (N.N. broj 198/03).



Shema 2. Grafički prikaz razvoja sustava tehničke zaštite

3. ZAHTJEVI I RJEŠENJA ZA DJELOVANJE SUSTAVA TEHNIČKE ZAŠTITE

U ovom poglavlju razrađene su vrste suvremenih sustava tehničke zaštite i sredstva koja se koriste u prvom zaštitnom pojasu – perimetru, a to su:

1. **Zaštitne ograde.**
2. **Sustav protuprovale.**
3. **Sustav video - nadzora.**
4. **Sustav kontrole pristupa.**
5. **Sredstva veze.**
6. **Zahtjevi i rješenja za djelovanje nadzornog centra.**

Za svaki od navedenih sustava tehničke zaštite i za sredstva koja se koriste u njihovoj potpori, a s ciljem ostvarenja tehničke zaštite štićenih prostora ili objekata u skladu sa:

- zahtijevanim mjerama tehničke zaštite pojedinih objekata i površina
- procjenom ugroženosti perimetra
- odgovarajućim shemama djelovanja
- određenim razinama zaštite,

potrebno je postaviti funkcionalne i tehničke zahtjeve, načela djelovanja i tehnička rješenja, sustave i pojedinu opremu u sustavu.

Tehnički zahtjevi

Tehnički zahtjevi za djelovanje sustava tehničke zaštite su:

- Sustav i oprema moraju zadovoljiti zahtjeve iz normi kao što su ISO 9001.
- Sustav mora biti modularan kako bi osigurao buduće dogradnje u skladu s potrebama.
- Prilikom ugradnje opreme voditi računa o preporukama proizvođača opreme.
- Sve vodiče za prijenos signala i napajanje na oba kraja zaštititi uređajima za prednaponsku zaštitu.
- Po programiranju sustava definirati pokusno razdoblje za rad sa sustavom tijekom kojega će se uočiti možebitne potrebe za izmjenama programskih parametara.

Funkcionalni zahtjevi

Funkcionalni zahtjevi za djelovanje sustava tehničke zaštite su:

- Sustave smiju ugrađivati i održavati samo ovlašteni djelatnici tvrtki koje imaju odobrenje za bavljenje djelatnošću tehničke zaštite.
- Zaštita osoblja i imovine u štićenom objektu ili prostoru.
- Popis funkcija koje pojedini sustavi zaštite moraju ispunjavati.
- Automatska i ručna promjena stanja nadzora nad javljačima i zonama.
- Sigurna i pouzdana detekcija.
- Sigurno funkcioniranje sustava bez obzira na vremenske okolnosti (kiša, snijeg, magla itd.).
- Velike mogućnosti potvrde uzroka alarma.
- Rano upozorenje/brzi odaziv.
- Moguć nadzor nad vrlo velikim površinama.
- Minimum lažnih alarma.
- Mali troškovi nadzora i održavanja.
- Jednostavna uporaba.
- Rad sa sustavom mogu obavljati samo osobe obučene za obavljanje ove djelatnosti.
- Programiranje sustava i izmjene na sustavu trebaju izvoditi isključivo osobe obučene kod proizvođača opreme.
- Uređaje i opremu koristiti sukladno s proizvođačevim uputama.

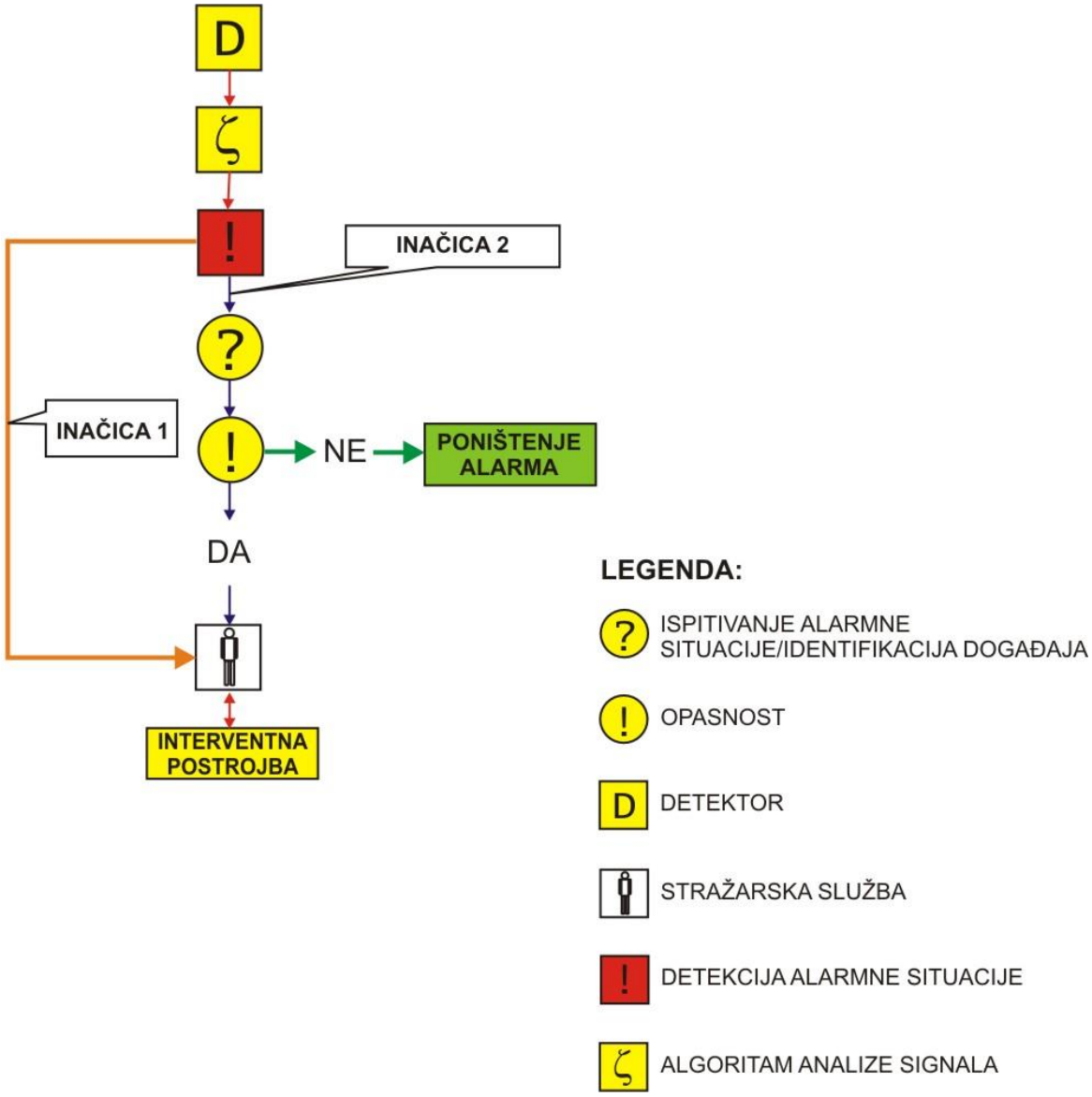
Načelo djelovanja sustava tehničke zaštite

Iz **sheme 3.** je vidljivo načelo djelovanja sustava tehničke zaštite. Organizacija sustava tehničke zaštite podrazumijeva upotrebu detektora s mogućnošću analize primljenog signala prema određenim kriterijima (u skladu s načinom rada detektorskog sklopa). Upotrebom takvih detektora postiže se značajno smanjenje broja lažnih alarma.

Nakon što je detektor signala ustanovio da su zadovoljeni kriteriji nastanka alarma, alarmna situacija se oglašava u nadzornom centru svjetlosno-zvučnim signalnim uređajima.

Sustavi tehničke zaštite se u osnovi razlikuju u tijeku odvijanja procesa nakon detekcije alarmne situacije.

U **inačici 1.** svjetlosno-zvučna signalizacija alarma prenosi se stražarskoj službi u nadzornom centru nakon čega ona alarmira interventnu postrojbu koja mora intervencijom na mjestu nastanka alarma identificirati događaj i odgovoriti u skladu s identificiranom situacijom.



Shema 3. Djelovanje sustava tehničke zaštite

Inačica 2. podrazumijeva postojanje uređaja ili sklopova sustava tehničke zaštite koji će osigurati ispitivanje i identifikaciju događaja, a da pri tome ne mora interventna postrojba izaći na mjesto događaja. Identifikacijom se nepobitno potvrđuje postojanje stvarne alarmne situacije ili utvrđivanje postojanja lažnog

alarma. U slučaju potvrde postojanja alarmne situacije interventna postrojba izlazi na mjesto nastanka alarma. U slučaju lažnog alarma, alarm se poništava.

U skladu s općim načelom djelovanja sustava tehničke zaštite izrađena su i načela djelovanja drugih sustava s tehničkim rješenjima.

3.1. Zaštitne ograde

Zaštitne ograde imaju zadaću, usporiti djelovanje potencijalnog počinitelja kaznenog djela u pokušaju prodora u zaštićeni prostor. Sukladno Pravilniku o uvjetima i načinu provedbe tehničke zaštite (N.N. broj 198/03), primjenjenim priznatim pravilima u provedbi tehničke zaštite, zahtjevi za zaštitne ograde su:

Tehnički zahtjevi

Tehnički zahtjevi koji se postavljaju pred zaštitne ograde su:

- Sustav i oprema moraju zadovoljiti zahtjeve iz normi ISO 9001.
- Sustav mora biti modularan kako bi osigurao buduće dogradnje sukladno potrebama (detektora, vodiča itd.).
- Prilikom ugradnje opreme voditi računa o preporukama proizvođača opreme.

Funkcionalni zahtjevi

Funkcionalni zahtjevi koji se postavljaju pred zaštitne ograde su:

- Spriječiti nekontrolirani ulaz i zaštititi osoblje i imovinu u štićenom objektu ili prostoru.
- Omogućiti otkrivanje i sprečavanje pojava koje mogu nanijeti štetu osobama ili imovini u štićenom prostoru.
- Omogućiti kontrolirani pristup osoba i vozila na, za tu namjenu određenim mjestima.
- Sustav mora omogućiti dogradnju sukladno potrebama, npr. detektora, vodiča.

Načelo djelovanja

Ograda se smatra prvim i najjednostavnijim stupnjem zaštite u svakom sustavu za zaštitu perimetara. Prema ispitivanjima koje su provele vladine agencije u SAD-u, obučeni i opremljeni diverzanti višeg stupnja vještine mogu presjeći žičanu ogradu u roku od 18 sekundi, a preskočiti je ili se provući ispod nje u roku od 5 sekundi.

Osnovno načelo djelovanja zaštitne ograde je da potencijalnom provalniku ili diverzantu pomoću fizičke barijere (ograde) **uspori** njegovo djelovanje. Fizičku barijeru predstavlja:

- visina ograde
- oblik njene izvedbe
- materijal od kojeg je izgrađena (zid, žičana mreža, istegnuti metal, žica itd.).

Razne vrste detektora koji se ugrađuju na tlu ispred zaštitne ograde ili koji se ugrađuju na samu ogradu, te sustav video nadzora omogućuju stražarima 24 satni nadzor stanja zaštitne ograde bez obzira bilo to noću ili danju, u složenim meteorološkim uvjetima (kiša, snijeg, magla).

Osnovna je uloga zaštitne ograde usporavanje prodora (provalnika, diverzanta) i pošto je ona integrirana sa sustavima za otkrivanje i dojavu alarma (sustav protuprovale, sustav video nadzora), omogućuje stražarima i stražarskim službama nadzor i pravovremenu intervenciju nakon dojave alarma, a samim tim i zaštitu štićenih objekata i površina.

Tehničko rješenje zaštitne ograde

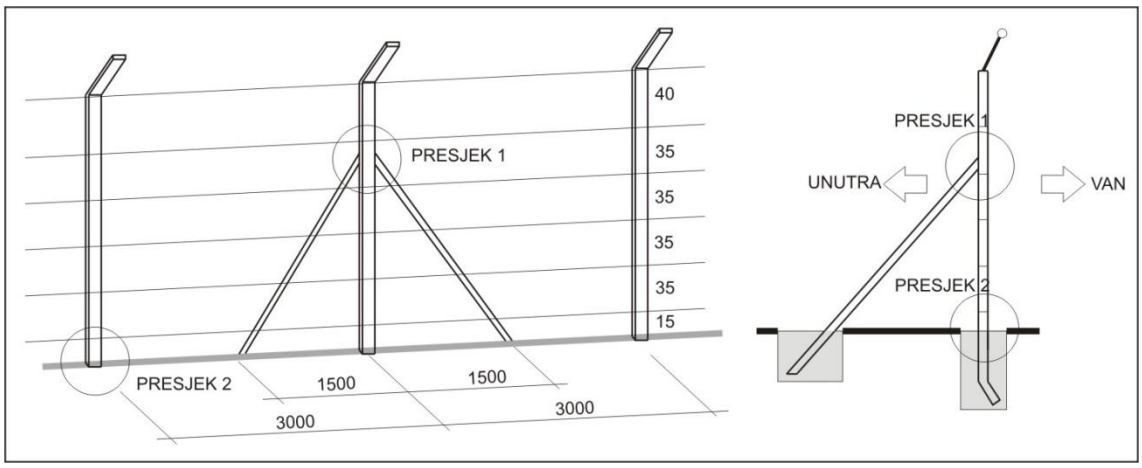
Tehničko rješenje zaštitne ograde ovisi o: stupnju sigurnosti koji mora pružiti zaštitna ograda, vrsti materijala od kojeg je izrađena i načinu postavljanja žičanih prepreka.

Za izradu perimetarskih ograda koriste se različiti materijali, pa ograde mogu biti:

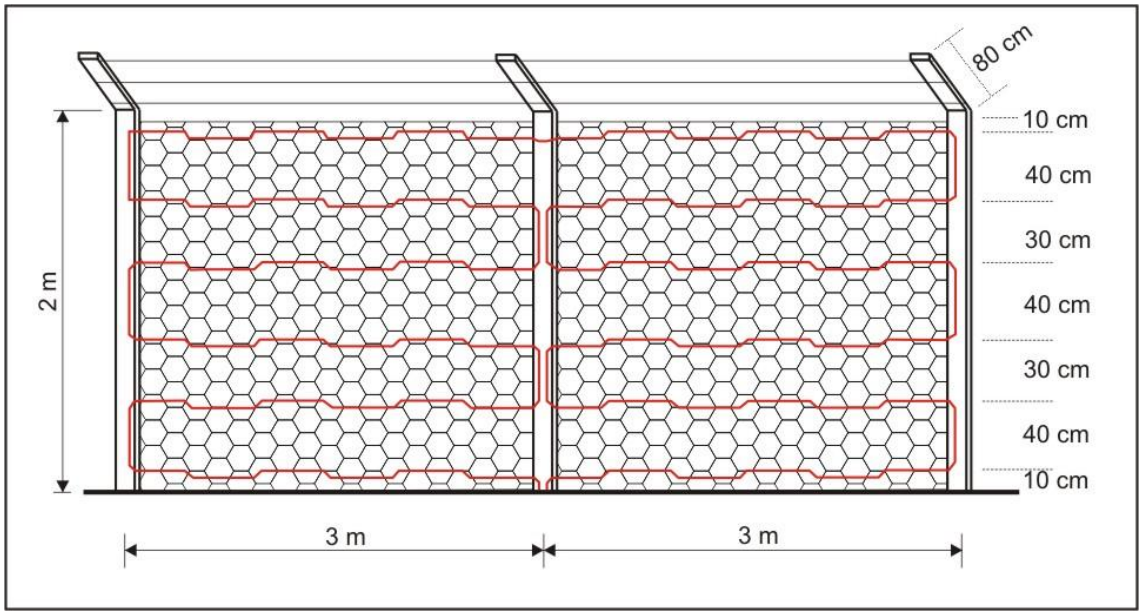
- zidane ograde (opeka, betonski blokovi, betonski elementi)
- ograde od krutog žičanog pletiva
- ograde od bodljikave žice itd.

Ograde mogu nositi betonski ili metalni stupovi te mogu biti različitih visina.

Za zaštitu objekata najčešće se koristi žičano pletivo koje se učvršćuje na betonskim ili metalnim stupovima na međusobnoj udaljenosti od 3 metra. S unutrašnje strane ograda se pojačava kao što je vidljivo na slici 4. Visina ograde je 2 metra, dok je gornji krak ograde, koji je usmjeren prema vanjskom djelu perimetra, dužine 60 do 80 centimetara i pod kutom od 60 do 80° (slika 5.).

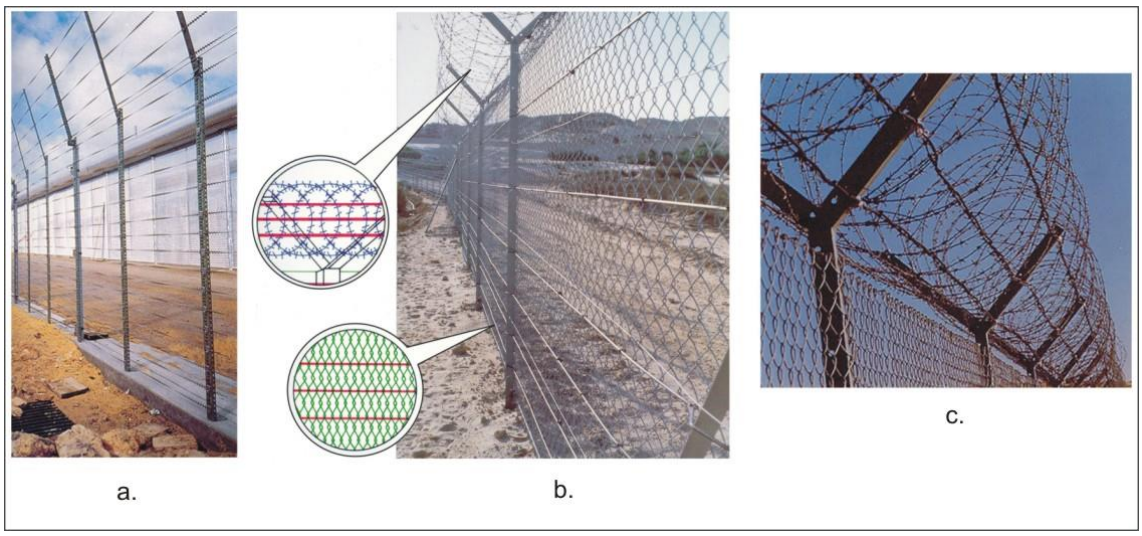


Slika 4. Ojačavanje ograde



Slika 5. Izgled ograde izrađene od žičanog pletiva s betonskim ili metalnim stupovima

Gornji krak ograde koji je okrenut prema vanjskom dijelu perimetra vrlo se često štiti s nekoliko redova bodljikave žice (slika 6a.). Gornji krak zaštitne ograde može biti izrađen i u obliku slova “V”, s time da se s gornje strane učvrsti bodljikava žica kružnog oblika (slika 6b i 6c.).



Slika 6. Načini postavljanja bodljikave žice na ogradu

Da bi se povećao stupanj sigurnosti koji pruža ograda, potrebno je povećati sigurnost javljačkim sustavom za njezin nadzor. Jedan od takvih sustava koji je projektiran za zaštitu perimetra, odnosno nadzor ograde je i sustav kod kojeg detektor dojavljuje mehaničke vibracije koje se generiraju na žičanoj ogradi pri penjanju preko nje, provlačenju ispod, rezanju ograde ili slično (Slika 7.)

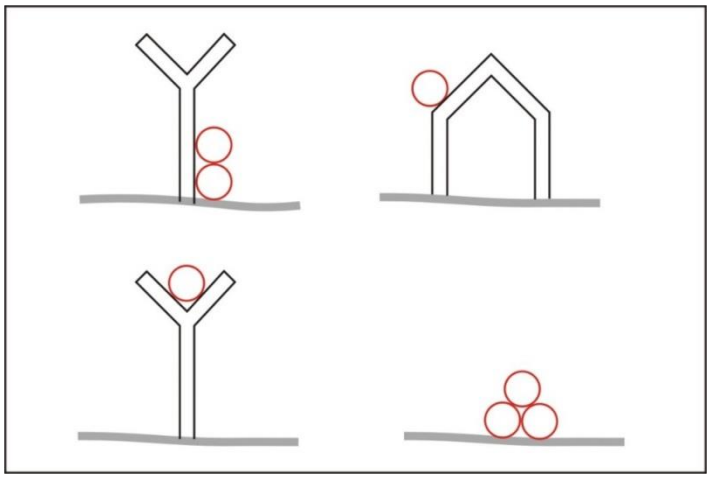
Slika 7. Prikaz načina postavljanja senzorskog vodiča na ogradu

Postoje detektori koji reagiraju na zvuk (slika 8.) i mnoge druge vrste detektora o kojima se govori u točci 6.5.2.

Slika 8. Detektori koji reagiraju na zvuk

Za zaštitne ograde od izuzetnog je značaja da se redovito održavaju, koriste i nadziru, sukladno uputama propisanim kako od proizvođača tako i projektanata i samih korisnika sustava zaštite. Osobitu pozornost posvetiti prilazima ogradi (perimetru) kako s vanjske tako i s unutarnje strane, da se održava čistim, lako pristupačnim, da se odstrani drveće i grmlje u neposrednoj blizini ograde, da se spriječi nastajanje lažnih alarma (zbog udara grana po ogradi) ili smanjenja vidljivosti (ometa rad video-nadzora).

Na slici 9. prikazan je način postavljanja žičanih prepreka uz ogradu, na ogradi, na objektu ili samostalno.



Slika 9. Načini postavljanja žičanih prepreka

3.2. Sustav protuprovale

Sustavi protuprovale spriječavaju potencijalnog počinitelja kaznenog djela, dojavom pokušaja prodora ili kretanja u zaštićenom prostoru. Sukladno Pravilniku o uvjetima i načinima provedbe tehničke zaštite (N.N. 198/03), primjenjenim priznatim pravilima u provedbi tehničke zaštite, zahtjevi za sustave protuprovale su:

Tehnički zahtjevi

Tehnički zahtjevi za djelovanje sustava protuprovale su:

- sustav i oprema moraju zadovoljiti zahtjeve iz normi ENV 50130, ENV 50131 ili strože
- sustav mora biti moduliran kako bi osigurao buduće dogradnje u skladu s potrebama
- napajanje sustava mora biti tip A (ENV 50131).

Funkcionalni zahtjevi

Funkcionalni zahtjevi za djelovanje sustava protuprovale su:

- Sustav mora sadržavati samo one detektore koji su pogodni za određenu okolinu i primjenu. Signal provale i poruka o provali moraju biti generirani, kada je detektor u aktivnom stanju kroz zadani period.
- Odabranim detektorima mora se mijenjati osjetljivost (detektori s aktivnim komponentama).
- Detektori za detekciju kretanja moraju imati sposobnost detekcije osjetnog smanjenja štićenog područja.
- Primjena područja pokrivanja mora biti omogućena samo ovlaštenim osobama. Neovlašteno podešavanje mora se detektirati i prijavljuje se kao sabotaža.
- Sustav mora imati sposobnost prepoznavanja sljedećih tehničkih pogrešaka:
  - generalna pogreška
  - pogreška napajanja
  - pogreška rezervnog napajanja
  - pogreška sustava za slanje alarma.

- Sustav mora imati minimalno četiri razine pristupa funkcijama:
  - razina 1 – pristup bilo koje osobe
  - razina 2 – pristup bilo kojeg korisnika
  - razina 3 – pristup servisnog osoblja
  - razina 4 – pristup proizvođača/ovlaštenog instalatera.
- Pristup funkcijama ograničen je pristupnim kodom.
- Uključenje sustava u aktivno stanje mora se izvoditi po strogo propisanoj proceduri. Mora postojati indikacija uspješno izvršenog uključenja. Uključenje se odbija, ukoliko detektori kretanja detektiraju osjetno smanjenje štićenog prostora.
- Isključenje sustava ili dijela sustava mora se ostvariti po strogo propisanoj proceduri pomoću autorizacijskog koda. Ako se pri isključenju ulazi u štićenu zonu, kretati se smije samo po strogo određenim pravilima. U tom slučaju dopušta se maksimalno vrijeme od 45 sekundi za provedbu kompletne procedure isključenja ili manje ovisno o stvarnim potrebama kretanja i isključenja. Ako se proces isključenja ne izvrši u zadanom periodu oglašava se alarm. Uspješno isključenje mora se indicirati svjetlosno-zvučnom signalizacijom.
- Sustav mora periodično komunicirati sa svim komponentama u svrhu provjere ispravnosti rada.
- Sustav mora nadzirati međuveze za komunikaciju.
- Promjena napajanja s primarnog na alternativno ne smije izazvati alarm, ali mora imati svjetlosno-zvučnu signalizaciju ispada primarnog napajanja.
- Sustav mora imati alternativno napajanje kapaciteta 24 Ah.
- Sustav mora imati mogućnost spajanja s ostalim sustavima preko PC-a.
- Sustav mora imati mogućnost prikaza na grafičkom sučelju s ucrtanim mapama raspoređenim u više razina ovisno o stupnju potrebnih detalja za precizno određenje mjesta nastanka alarma. Na mapama se mora nalaziti točan raspored detektora, prikazan jednoznačno određenim simbolom s mogućnošću dinamičke promjene boje simbola u skladu s vrstom primljenog alarmnog signala (alarm, sabotaža, tehnička pogreška).
- Sustav mora osigurati hijerarhijski pristup programiranju, parametriranju, upravljanju i otvaranju uređaja/sustava.

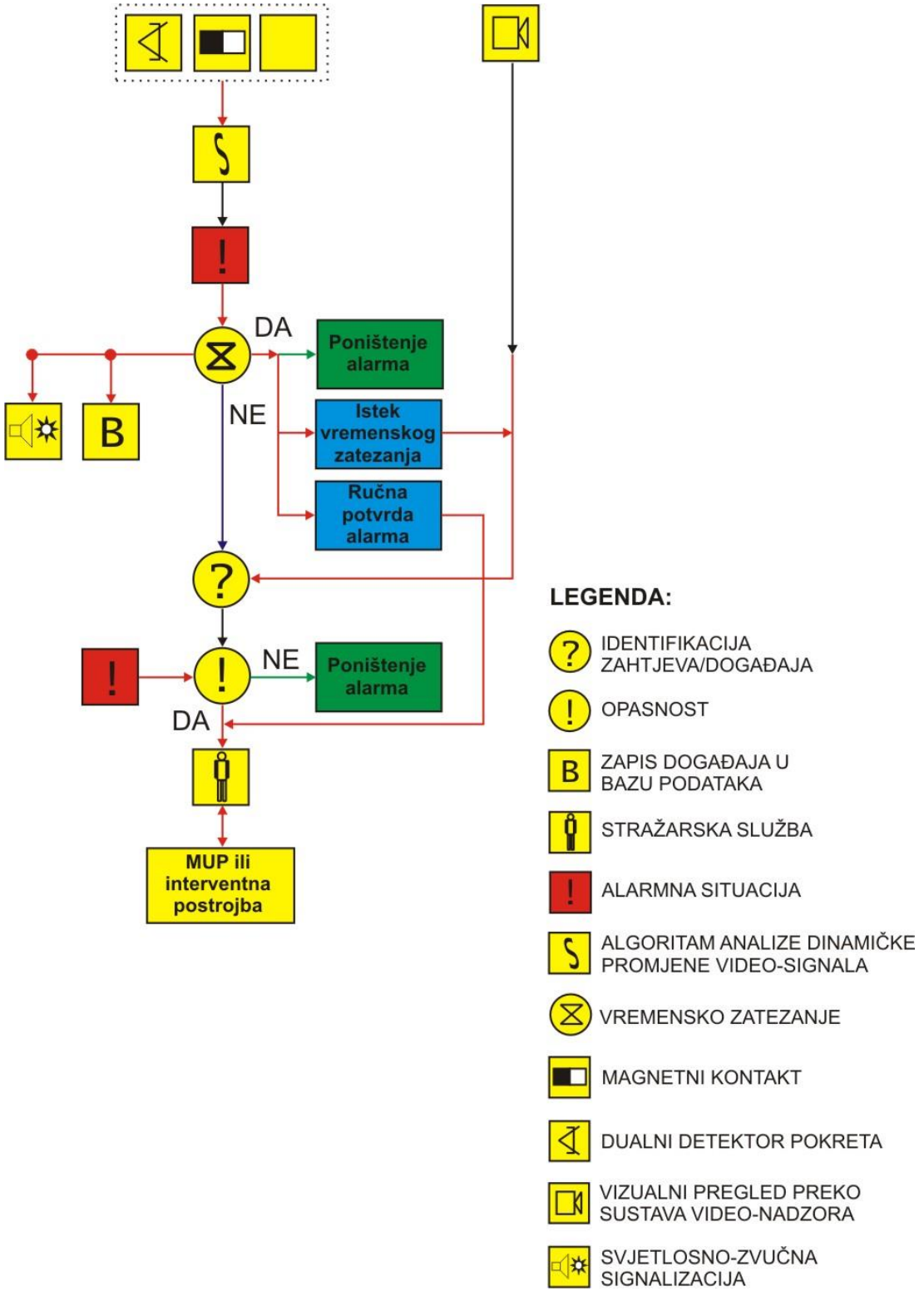
Načelo djelovanja sustava protuprovale

Djelovanje sustava protuprovale očituje se primjenom takvih detektora koji u sebi sadrže mikroprocesorski sklop za analizu signala u skladu s načinom primjene, vidi shemu 4. Detektor preko algoritma za analizu signala utvrđuje jesu li zadovoljeni zadani kriteriji za indikaciju alarma, ako jesu, signal alarma prosljeđuje se u nadzorni centar i utvrđuje se postojanje vremenskog kašnjenja.

Ako je za danu zonu predviđeno vremensko kašnjenje, čeka se istek vremenskog kašnjenja odnosno odgovarajuća reakcija unutar tog vremenskog intervala – ručna potvrda alarma ili poništenje alarma. U slučaju ručne potvrde alarma osoblje stražarske službe poduzima odgovarajuće mjere.

Po isteku vremenskog kašnjenja ili u slučaju da ono nije ni predviđeno, nakon oglašavanja alarmnog događaja, identificira se događaj u svrhu utvrđivanja je li alarm pravi ili lažni. U tu svrhu mogu se koristiti drugi detektori ili video - sustav. U slučaju iniciranja alarma s drugog detektora ili identifikacije alarmne situacije preko video sustava oglašava se opasnost i osoblje stražarske službe u sprezi s interventnom postrojbom ili MUP-om poduzima odgovarajuće mjere.

Osim protuprovale na objektu je predviđena dogradnja protuprepadnih elemenata. Alarm prepada se prenosi do centra i zahtijeva intervenciju osoblja stražarske službe.



Shema 4. Djelovanje sustava protuprovale

Tehničko rješenje sustava protuprovale sastoji se od:

1. Detektora protuprovale koji su raspoređeni po prostoru u skladu s načinom detekcije.
2. Centralnog procesorskog uređaja koji obrađuje signale pristigle s detektora.
3. Tipkovnice za upravljanje sustavom protuprovale.
4. Uređaja lokalnog signaliziranja.
5. Uređaja za prijenos signalizacije na udaljeno mjesto dojave.
6. Uređaja dozvole pristupa i upravljanja centralnim uređajem ili zaštitnim sustavom.
7. Elemenata protusabotažne zaštite.
8. Zahtjeva za napajanje.

1. Detektori su osnova svakog zaštitnog tehničkog sustava kojima se dojavljuje pokušaj prodora ili kretanje u zaštićenom prostoru. Zaštitni sustavi koriste detektore različitih namjena, različitih tehnologija, uvjeta ugradnje i načela na kojima se temelji detekcija prodora ili kretanja. Vrste detektora koji se najčešće koriste u zaštiti perimetra:

a) **Kontaktni detektori** (mehanički prekidači, magnetski prekidači, balansirani magnetski detektori). Primjenjuju se za zaštitu i kontrolu od neovlaštenog pokušaja odstranjivanja ili promjene položaja nekog elementa uključenog u zaštitni sustav. Reagiraju kao posljedica promjene položaja dijela kontaktnog detektora, a reakcija se ostvaruje zatvaranjem ili otvaranjem električnog kontakta. Uzrok promjene položaja električnog kontakta može biti magnetsko polje ili mehaničko djelovanje. U praksi su najprimjenjiviji magnetski kontakti.

b) **Detektori vibracija zida** ugrađuju se na konstrukcije (zidove, stropove, podove) a zadaća im je da detektiraju mehaničke vibracije prouzročene sječenjem, rezanjem, bušenjem, probijanjem ili bilo kakvom vrstom fizičkog prodora. Montirani detektori svojim piezoelektričnim ili mehaničkim pretvaračima, pretvaraju vibracije u električke veličine. Signal se šalje kroz filtar koji utvrđuje poklapa li se spektar detektiranog signala sa spektrom karakterističnim za pokušaj prodora. Ako se poklapa, uključuje se alarm.

c) **Pasivni infracrveni detektori** toplinsku energiju koju zrači okolni prostor posredstvom optike usmjerava na toplinski senzor. Svaku promjenu toplinskog stanja energije okolnog prostora, koja je na dohvatu optike detektora. Detektor signal šalje ugrađenom procesoru koji procjenjuje i

eventualno generira alarm. Rad pasivnih infracrvenih detektora temelji se na razlici temperature objekta i okoline.

d) **Ultrazvučni detektori** koriste se u "prostornoj zaštiti" kao detektori kretanja unutar nekog štićenog prostora. Detekcija se zasniva na promjeni frekvencije reflektivnog (odbijenog) zvuka od objekta koji se kreće. Detektor mora imati ultrazvučni predajnik i prijamnik. Prednost su im neosjetljivost na toplinu i lakoća zadržavanja njihove energije u odabranom prostoru. Ultrazvuk ne prolazi kroz zidove.

e) **Mikrovalni detektori** sadrže predajnik i prijamnik koji rade u X (rendgenskom) području. Mikrovalni detektori su uređaji za detekciju pokreta koji zrače električno polje u određenu zonu. Pokret u toj zoni remeti polje i prouzrokuje alarm. Mogu se koristiti u zatvorenim i otvorenim prostorima.

f) **Detektori s fotoelektičnom zrakom** koriste se za zaštitu vanjskih i unutarnjih prostora. Ovi detektori emitiraju zraku infracrvenog svjetla prema udaljenom prijamniku stvarajući tako "elektronički ogradu", koja je nevidljiva prostim okom jer je odabrana frekvencija svjetla iz područja nevidljivog dijela spektra. Detektor se sastoji od dvije komponente, predajnika i prijamnika, koji mogu biti udaljeni do 350 metara, a put zrake može se promijeniti zrcalima kako bi se postigla manje predvidljiva zapreka. Ako se najmanje 90% odaslanog signala ne primi u trajanju dužem od 75 mikrosekundi, uključuje se alarm.

g) **Detektori dvostruke tehnologije** ako se koriste detektori koji u jednom javljanju koriste dvostruko načelo detekcije kretanja, postiže se veća pouzdanost zaštite prostora. U jednom kućištu detektora nalaze se dva detektora koji rade na različitom načelu detekcije. Za alarm detektora potrebna je istovremena pobuda oba ugrađena detektora.

h) **Videodetektori pokreta** temelje se na videodetekciji pokreta i koriste sustave zatvorene televizije (CCTV) bilo ove optičke, bilo niske razine osvjetljenja, bilo infracrvene, za pružanje mogućnosti detekcije prodora, kao i za procjenu vjerodostojnosti alarma kojeg daje stražarsko osoblje. Sustavi zatvorene televizije pružaju i mogućnost dokumentiranja tijeka upada. Postoji mogućnost uspoređivanja trenutne scene s prethodno snimljenom slikom "praznog" područja. Za vanjsku zaštitu objekata i površina mogu se koristiti i

druge vrste detektora i i različitih barijera, ali ove prethodno navedene najzastupljenije su u praksi.

2. **Centralni procesorski uređaj** obrađuje prikupljene podatke te na osnovi njih daje nalog za aktiviranje lokalne signalizacije i prosljeđuje signal na udaljeno mjesto dojave. Uređaj nadzire i ostale uređaje zaštitnog sustava i komunicira s njima.

   U suvremenim sustavima tehničke zaštite susrećemo razne vrste centralnih uređaja, koji se međusobno razlikuju generacijski, koncepcijski i namjenski.

   Vrste centralnih uređaja:

   - klasični centralni uređaji
   - mikroprocesorski centralni uređaji za rad s klasičnim detektorima
   - mikroprocesorski centralni uređaji za rad s adresabilnim detektorima.

   Centralni uređaj s detektorima povezan je linijom kojom se razmjenjuju informacije u oba smjera: od centralnog uređaja do detektora ili drugih perifernih jedinica i obratno. Centralni uređaj omogućuje prikaz promjene stanja zaštitnog sustava na numeričkim displejima. Uređaji mogu imati na sebi ugrađene printere ili postoji mogućnost priključka printera na uređaj. Centralni uređaj zaštitnog sustava omogućuje povezivanje s centralnim nadzornim sustavom čitavog štićenog objekta ili površine.

3. **Tipkovnica za manipuliranje sustavom protuprovale** ugrađuje se u pult nadzornog centra. Služi za upravljanje sustavom protuprovale.

4. **Uređaji lokalnog signaliziranja,** suvremeni oblici alarmnih signalizatora čine kombinaciju alarma sirene i svjetlosnog signalizatora. Svjetlosni signalizatori pri alarmu najčešće svijetle isprekidanim svjetlom koje ostaje svijetliti i nakon prestanka rada zvučnog alarma, sve do poništenja alarma na centralnom uređaju. Iz sigurnosnih razloga zvučno svjetlosni signalizatori koriste autonomno napajanje.

5. **Uređaji za prijenos signalizacije na udaljeno mjesto** razlikujemo nekoliko načina prijenosa signalizacije na udaljeno mjesto dojave, što ovisi o načinu intervencije ili organizacije intervencije, mjestu dojave i važnosti sustava tehničke zaštite, a to su:

   - prijenos signalizacije uz korištenje iznajmljene telefonske parice – “poprečna veza”
   - prijenos signalizacije na pojedine telefonske adrese
   - prijenos signalizacije na centre nadzora i intervencije.

6. **Uređaji dozvole pristupa i upravljanja centralnim uređajem ili zaštitnim sustavom** pristup centralnom uređaju ili upravljačkom sustavu mora biti kontroliran i dopušten samo ovlaštenim osobama. Pristup se može nadzirati najjednostavnijim električnim kontaktnim bravama, do upravljačkim uređajima s tastaturama odabira šifre za dozvolu upravljanja i pristup, do programskih koraka, što ovisi o važnosti i složenosti zaštitnog sustava.
7. **Elementi protusabotažne zaštite,** pristup do priključnica ili elektronike mora biti kontroliran, odnosno može biti dopušten samo određenim osobama uz prethodno isključenje zaštite tog dijela zaštitnog sustava. Elementi protusabotažne zaštite su razni oblici mikrokontakata, mehaničkih ili magnetskih. Pokušaj otvaranja određenog kućišta ili dijela uređaja izaziva prosljeđivanje signalizacije neovlaštenog pristupa.
8. **Zahtjevi za napajanje,** primarno napajanje je 230 V/50 Hz. Zbog sigurnosnih razloga potrebno je predvidjeti alternativno napajanje svih uređaja. Alternativno napajanje (koriste se akumulacijske baterije) mora osigurati autonomiju 24 sata. Na periferiji se mogu koristiti izvori napajanja iz pojedinih objekata, s osiguranjem alternativnog napajanja potrebnog kapaciteta, pri čemu izvori primarnog i alternativnog napajanja moraju biti osigurani od sabotaže.

3.3. Sustav video-nadzora

Sustavi video-nadzora odvraćaju potencijalnog počinitelja kaznenog djela, detektiraju kretanje osoba ili objekta u štićenom prostoru, prepoznavaju poznate osobe u prostoru, važan su izvor podataka o počiniteljima kaznenih dijela i u suštini trebaju omogućiti njihovo prepoznavanje i identifikaciju. To je posebno važno za poslovne subjekte koji su prema odredbama Zakona o minimalnim mjerama zaštite u poslovanju gotovim novcem i vrijednostima (N.N. 173/03,150/05) obvezni imati sustav video-nadzora, te ga ugraditi i koristiti sukladno odredbama Zakona o privatnoj zaštiti (N.N. 68/03,139/10) i Pravilnika o uvjetima i načinu provedbe tehničke zaštite (N.N. 198/03).

Tehnički zahtjevi

Tehnički zahtjevi za djelovanje sustava video-nadzora su:

- Sustav i oprema moraju zadovoljiti zahtjeve iz normi ENV.
- Sustav mora biti modularan kako bi osigurao dogradnju u skladu s mogućom prenamjenom pojedinih prostora.
- U svrhu dobivanja adekvatnog osvjetljenja nadziranog područja, tamo gdje je to potrebno, osigurati dodatnu rasvjetu.
- Komunikacija kamera – centar mora se ostvariti preko optičkih kabela i optoelektričnih pretvornika.

Funkcionalni zahtjevi

Funkcionalni zahtjevi za djelovanje sustava video-nadzora su:

- Sustav treba osigurati praćenje aktivnosti u nadzornom centru na manjem broju monitora, kako bi se ostvarila puna pažnja osoblja u centru.
- U detekciji pokreta osigurati rano upozorenje/brzi odziv.
- U svrhu postizanja što brže obrade video-signala pri detekciji pokreta treba predvidjeti upotrebu jednog mikroprocesorski upravljanog sklopa za analizu video-signala za svaku kameru.
- Zone detekcije ne smiju biti duže od 80 metara.
- Sustav mora imati svojstvo virtualnog trodimenzionalnog proračunavanja perspektive za nadzor 2D i 3D objekata, odnosno svojstvo percepcije 3D slika.
- Mora biti omogućeno postavljeno parametara detekcije pokreta neovisno za svaku kameru kao i grupiranje više kamera putem aplikacijskih programa.
- Parametriranje detekcije pokreta mora omogućiti minimalno definiranje većeg broja zona osjetljivosti u slici podesivo po veličini zone, brzinu i smjer kretanja u zoni, veličinu objekta koji će izazvati alarm.
- Sustav mora imati mogućnost eliminiranja lažnih alarma odnosno alarma koji nastaju zbog pomicanja granja ili grmlja, promjene osvjetljenja, loših vremenskih prilika.
- Obrada, analiza i pohrana video - signala mora biti digitalna.
- Pohrana video signala alarmnih slika s kolor grafičkim mapama za lociranje mjesta nastanka alarma.
- Video signali se pohranjuju privremeno i trajno s mogućnošću čuvanja arhiviranih medija do 15 dana.
- Sustav mora tretirati odvojeno signal alarma, signal sabotaže i signal tehničke pogreške.

- Sustav mora biti upravljiv s PC-a.
- Sustav mora imati mogućnost prikaza na grafičkom sučelju s ucrtanim mapama raspoređenim u više razina ovisno o stupnju potrebnih detalja za precizno određenje mjesta nastanka alarma. Na mapama se mora nalaziti točan raspored detektora/kamera, prikazan jednoznačno određenim simbolom s mogućnošću dinamičke promjene boje simbola u skladu s vrstom primljenog alarmnog signala (alarm, sabotaža, tehnička pogreška).
- Sustav mora osigurati generiranje uputa osoblju stražarske službe u ovisnosti o vrsti alarmne situacije.
- Sustav mora osigurati hijerarhijski pristup programiranju, parametriranju, upravljanju i otvaranju uređaja/sustava.

Načelo djelovanja sustava video-nadzora

Predviđeno je da osim standardne opreme video-nadzora (kamera, objektiva, monitora, uređaja za snimanje, instalacija, itd.) sustav posjeduje sklop i algoritme potrebne za analizu video-signala i prepoznavanje kretanja.

Načelo djelovanja sustava video-nadzora, vidi shemu 5., nakon što je video-signal primljen, u nadzornom centru vrši se analiza signala i u slučaju zadovoljenja kriterija promjene, oglašava se alarm. Iz memorije za privremenu pohranu, zajedno s alarmnim slikama trajno se pohranjuju predalarmne slike (u skladu s odabranim parametrima). Istovremeno se oglašava svjetlosno-zvučno upozorenje, slika se predočava na monitoru i u bazu podataka pohranjuju informacije o događaju.

Potom se ispituje alarmna situacija i identificira događaj. U slučaju potvrde alarma od drugih uređaja ili sustava, osoblje stražarske službe intervenira na mjesto događaja i obavješćuje interventnu postrojbu.

Karakteristike sustava video-nadzora za novčarske institucije

Člankom 5. Zakona o minimalnim mjerama zaštite u poslovanju gotovim novcem i vrijednostima, novčarske su institucije zbog ostvarivanja minimalnih sigurnosnih uvjeta zaštite, svrstane u tri kategorije:

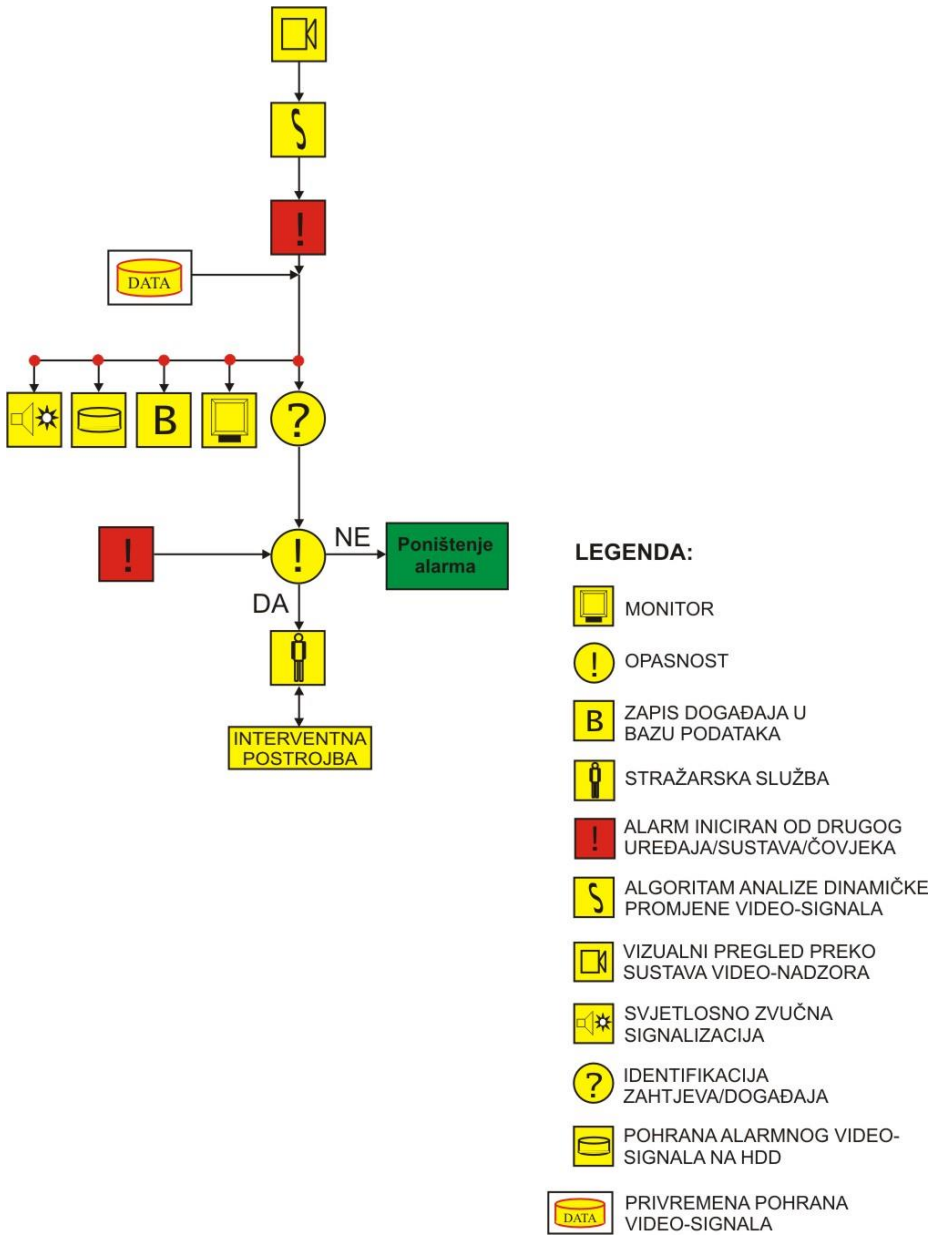
- Prva kategorija: Hrvatska narodna banka, poslovnice FINA-e, banke, stambene štedionice i poštanski uredi Hrvatske pošte.
- Druga kategorija: mjenjačnice, poslovnice Hrvatske lutrije, kladionice i štedno-kreditne zadruge.
- Treća kategorija: bankomati.

Odvraćanje potencijalnog počinitelja kaznenog djela postiže se isticanjem upozorenja da je prostor štićen sustavom tehničke zaštite i vidljivim uređajima

(kamerama) u i ispred štićenog prostora. (Statistički podaci pokazuju da su kaznena djela počinjena prvenstveno nad objektima i prostorijama koji nisu štićeni).

Iz prve kategorije sve novčarske institucije imaju sustave video-nadzora, osim poštanskih ureda čije je instaliranje u završnoj fazi.

Iz prikaza kaznenih djela razbojništava (tablica 2.) novčarske institucije iz druge kategorije, kao što su mjenjačnice, gdje je prikazan porast kaznenih djela za 19%, kladionice za 760%, reagirala je i država koja je zakonskim odredbama propisala obvezu tehničke zaštite takvih institucija, propisala vrstu tehničkih sredstava te odredila točke ugroženosti takvih institucija.



Shema 5. Djelovanje sustava video-nadzora

Tehničko rješenje sustava video-nadzora

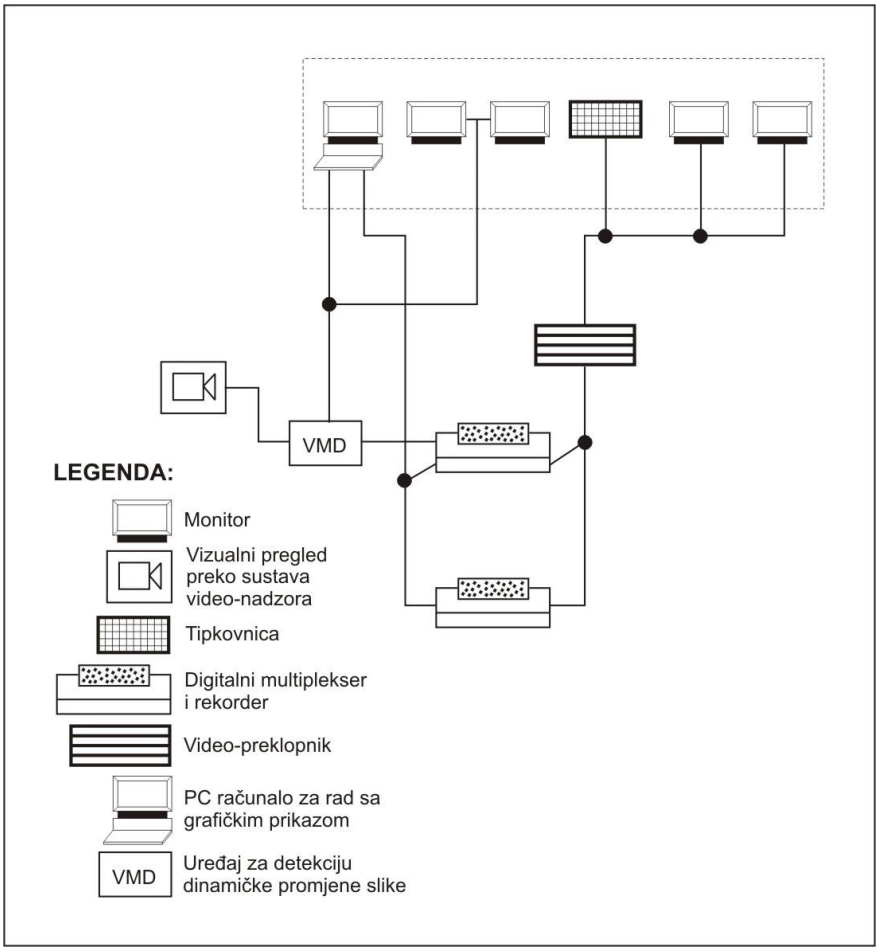
Sustavom video-nadzora potrebno je pokriti vanjski perimetar i unutrašnje prostore. U vanjskom perimetru postoje dijelovi lokacije s različitom kvalitetom odnosno razinom rasvjete. U unutrašnjim prostorima rasvjeta je zadovoljavajuće razine, ali je potrebno implementirati (ugraditi) automatsko daljinsko upravljanje rasvjetom.

Radi ostvarenja svih uvjeta i kakvoće slike, uvest će se sljedeći tipovi kamera:

1. Kamera za vanjsku montažu, C/B, visoke rezolucije, s pomaknutom karakteristikom prema IC području s IC reflektorom za primjenu u uvjetima slabe rasvjete – zaštita perimetra.
2. Kamera za vanjsku montažu, C/B visoke rezolucije, za primjenu u uvjetima dobre vanjske rasvjete – prostori s postojećom rasvjetom.
3. Kamera za unutrašnju montažu, kolor, visoke rezolucije, u zaštićenom kućištu.

Vanjske kamere spojene su na sofisticirani sustav detekcije pokreta preko video-matrice (prijeko potrebna zbog velikog broja kamera). Uređaji za detekciju pokreta u slučaju alarma prosljeđuju video-signal na digitalni multiplekser-rekorder koji pohranjuje video-signal (vidi shemu 6.). Video-signal se prosljeđuje na alarmni monitor koji pokazuje sliku. Istovremeno se oglašava svjetlosno-zvučni interni alarm, na grafičkom sučelju se prikazuje mapa s alarmnom kamerom u boji drugačijoj od boje kojom se prikazuje normalno stanje.

U svrhu naknadnog pretraživanja u sustavu se nalazi dodatni digitalni multipleksor-rekorder kako se sustav ne bi ostavio bez snimanja.

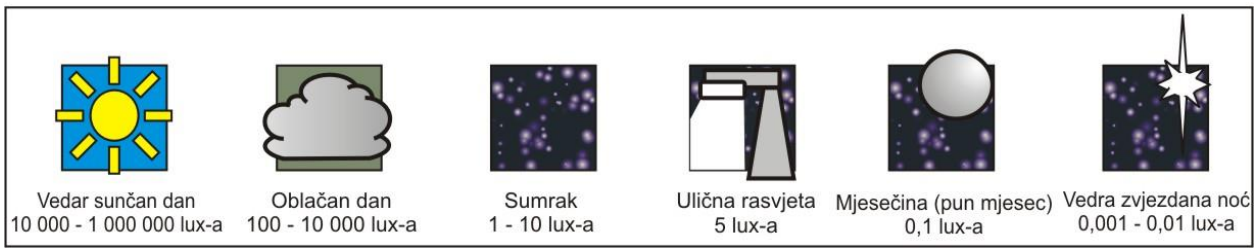


Shema 6. Tehničko rješenje sustava video-nadzora

Kamere

Prilikom odabira kamere treba znati:

- uvjete lokacije kamere
- razinu osvijetljenosti (slika 10.)
- rezoluciju kamere
- svrhu kamere.



Slika 10. Karakteristične razine osvjetljenja (10)

U odabiru crno-bijele ili kamere u boji treba uzeti u obzir potrebnu razinu prepoznavanja.

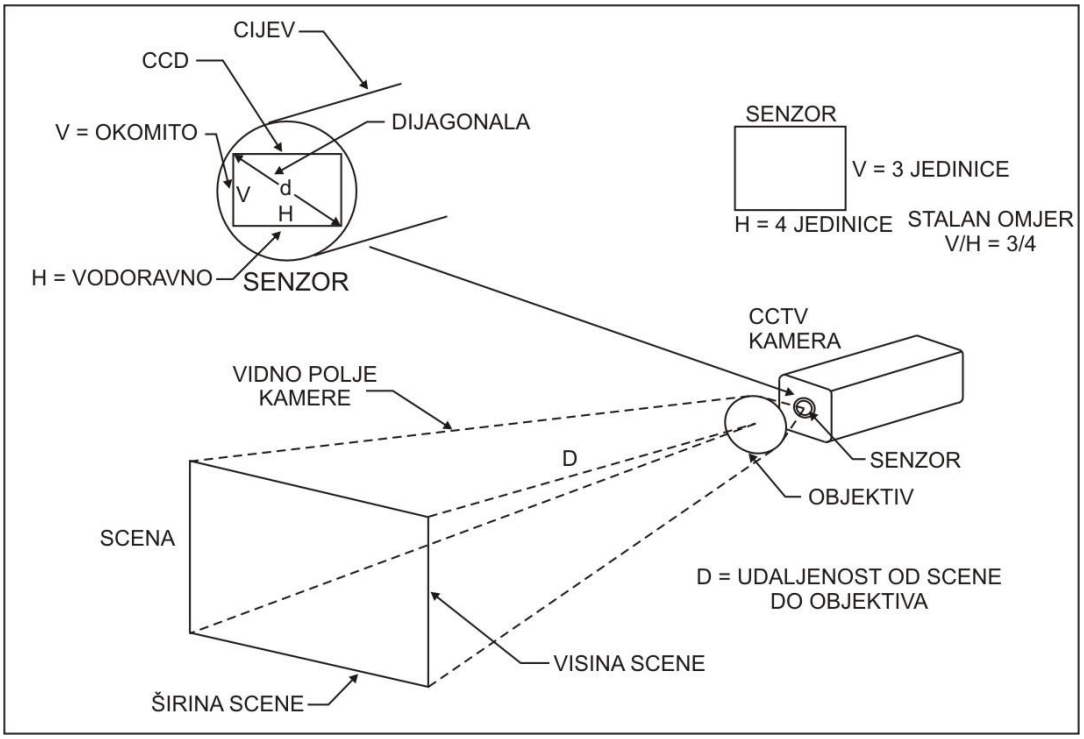
Kamere se s obzirom na minimalnu potrebnu količinu osvjetljenja mogu podijeliti na **kamere za opću upotrebu** koje normalno rade od danjeg svjetla do sumraka i na **kamere za noćno nadziranje** kojima je potrebna mala količina osvjetljenja (manja od 0,01 luxa), ali je za njih prijeko potreban objektiv s auto irisom da bi radile i pri danjem svjetlu. Bitna je i rezolucija kamere jer određuje kakvoću slike i mogućnost prepoznavanja detalja. Rezoluciju kamere treba uskladiti s rezolucijom monitora. Kamera male rezolucije dat će lošu kakvoću slike i na monitoru velike rezolucije. Kamere imaju i različite izlaze za upravljanje irisom. Neke podržavaju video tip irisa (izlaz iz kamere je video signal), a neke drive tip auto irisa (kamere s ugrađenim pojačalom i izravnim izlazom za monitore auto irisa). Treba obratiti pozornost na napajanje kamere ovisno o raspoloživom napajanju na lokaciji kamere.

Objektivi

Prije odabira objektiva potrebno je znati tip kamere, lokaciju, zahtjeve koji se postavljaju na kvalitetu slike i područje koje se snima.

Prilikom odabira objektiva treba uzeti u obzir sljedeće karakteristike objektiva:

1. **Format objektiva** može biti 1/3, 1/2, 2/3 i 1 kao i kod kamera. Format objektiva nikako ne smije biti manji od formata kamere.
2. **Tip montiranja C ili CS,** C tip montiranja određuje da kamera ima otvor promjera 1'' i udaljenost od kraja objektiva do senzora kamere 17,526 milimetara. Zbog smanjenja veličine kamere uveden je CS tip montiranja kod kojeg kamera ima isti promjer otvora, ali je udaljenost od kraja objektiva do senzora kamere 12,5 milimetara, tj. 5 milimetara manja. Zato treba odabrati objektiv koji ima isti tip montiranja kao kamera. C objektiv je moguće montirati i na CS kameru uz dodatak 5 milimetara odstojnika, dok se CS objektiv može montirati samo na CS kameru.
3. **Žarišna duljina objektiva** određena je veličinom vidnog polja i udaljenošću od kamere do snimanog objekta pri čemu treba uzeti u obzir format objektiva. Također je potrebno znati je li potrebno snimanje fiksnog vidnog polja ili će se vidno polje kamere mijenjati. To određuje da ćemo odabrati objektiv s fiksnom žarišnom duljinom ili zoom - objektivom čija se žarišna duljina može ručno ili automatski mijenjati u nekom rasponu, na primjer 10:1 (slika 11.)



Slika 11. Žarišna duljina objektiva

Žarišna duljina izračunava se nakon mjerenja vodoravne i okomite dimenzije željenog vidnog polja i udaljenosti objekta od kamere pomoću tablice (tablica 3.) ili posebnog alata za određivanje žarišne duljine.

Tablica 1. Tablica vodoravnog kuta vidnog polja s obzirom na žarišnu duljinu i format objektiva

ŽARIŠNA DULJINA	1/3''	1/2''	2/3''
2.8 mm	94°48''	-	-
4.0 mm	63°36''	-	-
4.8 mm	54°22''	69°00''	95°34''
6.0 mm	44°48''	58°00''	-
8.0 mm	32°36''	43°36''	58°41''
12.0 mm	22°32''	31°07''	-
12.5 mm	21°32''	28°43''	39°07''
16 mm	17°03''	22°37''	30°40''
25 mm	10°58''	14°35''	19°58''
50 mm	5°29''	7°19''	10°02''
75 mm	3°39''	4°53''	6°34''
100 mm	-	3°40''	5°01''

Odabir objektiva

Sljedeća formula omogućava brzo izračunavanje vodoravnog vidnog polja kamere i objektiva na određenoj udaljenosti:

$$\text{vodoravno vidno polje} = \frac{\text{vodoravna dimenzija chip - a x udaljenost}}{\text{žarišna daljina objektiva}}$$

$$\text{okomito vidno polje} = \frac{\text{okomita dimenzija chip – a x udaljenost}}{\text{žarišna daljina objektiva}}$$

Dimenzije chipa su konstante (tablica 4.):

Tablica 2.

FORMAT	VODORAVNA DULJINA	OKOMITA DULJINA
1/3''	4.4 mm	3.3 mm
1/2''	6.2 mm	4.8 mm
2/3''	8.8 mm	6.6 mm
1''	12.8 mm	9.6 mm

Primjer: koristeći kameru 1/3'' i objektiv 4 mm, na udaljenosti 10 metara imamo:

a) vodoravno vidno polje

$$\text{vodoravno vidno polje} = \frac{4.4 \text{ x } 10}{4} = 11\text{m}$$

b) okomito vidno polje

$$\text{okomito vidno polje} = \frac{3.3 \text{ x } 10}{4} = 8.25\text{ m}$$

Općenito, objektive s obzirom na žarišnu duljinu dijelimo na **širokokutne, normalne, teleskopske (uskokutne) i zoom objektive.** Širokokutni objektiv ima malu žarišnu duljinu, veliko vidno polje, objekti su smanjene veličine i dobivena slika je manje rezolucije. Normalni objektivi imaju žarišnu duljinu kao ljudsko oko, tj. za objektiv 1'' normalna žarišna duljina je 25 milimetara (za 2/3'' 16 milimetara, za 1/2'' 12.5 milimetara i za 1/3'' 8 milimetara). Manje vrijednosti od navedenih znače širokokutni objektiv, a veće vrijednosti teleskopski. Teleskopski objektivi povećavaju i približavaju udaljeni objekt, ali je vidno polje malo. Zoom objektivi imaju promjenjivu žarišnu duljinu od na primjer 11-110 milimetara te povećanje,

na primjer 1:10. To znači da s istim objektivom možemo promatrati veliko vidno polje u blizini kamere i po potrebi zumirati (povećavati) pojedini dio objekta. Zoom objektivi mogu biti s ručnim ili daljinskim upravljanjem. Obično je upravljanje zumom izvedeno zajedno sa zakretanjem kamere iz nadzornog centra tako da kamera pokriva veliko područje.

4. **Iris** je podesiva blenda smještena u cijevi objektiva i određuje količinu svjetlosti koja prolazi kroz objektiv do senzora kamere. Ako je osvjetljenje objekta malo, iris treba otvoriti, a ako je objekt jako osvijetljen iris treba zatvoriti u skladu s osjetljivošću senzora kamere. Iris se može podešavati ručnim okretanjem prstena na objektivu ili može biti automatski te motori sami otvaraju i zatvaraju iris s obzirom na video signal. Prilikom odabira objektiva s ručnim ili automatskim irisom treba znati hoće li se objektiv koristiti u aplikaciji s promjenjivim uvjetima osvjetljenja ili će osvjetljenje biti gotovo konstantno. Također treba znati vrstu kamere koje imaju ugrađeno podešavanje ovisno o razini osvjetljenja (*auto shutter*) tako da objektiv s automatskim irisom možda nije ni potreban. Objektivi s automatskim irisom mogu biti **"video"** i **"drive"** tipa. Video tip objektiva ima ugrađene motore i kontroler koji na osnovu video signala iz kamere određuje koliko se iris treba otvoriti ili zatvoriti. Objektiv tipa "drive" ima ugrađene samo motore dok je kontroler u kameri koja izravno šalje signale na motore auto irisa. Video signal za upravljanje auto irisom obično je određen sa srednjom vrijednosti osvjetljenja objekta, ali postoji i mogućnost da je video signal određen maksimalnim osvjetljenjem neke točke (pik) što se koristi kada je u vidnom polju osvjetljenje jednolično, ali su neke točke izrazito osvijetljene (na primjer svjetla automobila).
5. **F-stop ili f-broj** izražava koliko svjetla može ući u objektiv. To je također maksimalni otvor irisa. F-stop je određen omjerom žarišne duljine i promjera objektiva. Što je taj broj manji, objektiv može skupiti više svjetla i proizvesti kvalitetniju sliku. Ako je f1.2 brzi objektiv može koristiti uz nisku razinu osvjetljenja objekta (noćno snimanje). F-stop se također naziva i brzinom objektiva te je na primjer f1.2 brzi objektiv, a f4 spori. Zoom objektivi su, s obzirom da im se žarišna duljina mijenja, a promjer ostaje isti, brzi za širokokutni položaj i spori za teleskopski položaj.
6. **Fokus** određuje širinu slike. Postoje objektivi s fiksnim fokusom i prstenom za podešavanje fokusa. Ako je fokus fiksan moguće je fokusirati samo objekte dalje

od neke udaljenosti, dok se s podesivim fokusom mogu fokusirati objekti na različitim udaljenostima. Dubina polja je veličina područja ispred i iza objekta koje će biti fokusirano. Ako koristimo zoom objektive, potrebno je pri instalaciji podesiti fokus u nekoliko koraka – postaviti prsten za podešavanje fokusa na "daleko" sa zoomom podešenim na širokokutno pokrivanje, usmjeriti kameru na objekt udaljen 30 do 550 metara i podesiti fokus kamere za maksimalnu oštrinu, a zatim zumirati na objekt u neposrednoj blizini (*close up*) i ponovo podesiti fokus za maksimalnu oštrinu. Nakon ovog postupka bit će moguće postići zumiranje *in* i *out* kroz cijelo polje pokrivanja uz tako definiranu poziciju prstena za fokusiranje.

7. **Specijalni objektivi** su razvijeni za razne specijalne aplikacije, a postoje različiti tipovi specijalnih objektiva:
   a) **Pinhole objektivi** imaju mali promjer vrha objektiva i namijenjeni su za skrivenu ugradnju. Pinhole* objektiv može biti ravan ili pod pravim kutom ovisno o raspoloživom prostoru za ugradnju kamere. Postoje razni oblici vrhova pinhole objektiva koji se odabiru ovisno o veličini i obliku otvora kroz koje će snimati.
   b) **Mini objektivi** se koriste uz minikamere također za skrivene aplikacije.
   c) **Objektivi s optičkim vlaknima** koriste se kada je potrebno da objektiv prolazi kroz otvor dug od nekoliko centimetara do nekoliko metara. Sastoje se od prednje leće za fokusiranje snimljene slike na snop optičkih vlakana koji prenose slike na stražnju leću, a ona ponovno stvara sliku i fokusira je na senzor kamere.
   d) **Asferični objektivi** koriste se kada je potreban širokokutni objektiv s velikom optičkom brzinom i malom distorzijom (izobličenjem slike). Asferični objektivi zbog oblika leće skupljaju više svjetlosti nego klasični objektivi sa sferičnim lećama te se mogu koristiti kod malog osvjetljenja objekta.
   e) **Objektivi s dijeljenjem slike** mogu imati 2 ili 3 ulazne leće različito usmjerene te se proizvedena slika sastoji od 2 ili 3 slike iz različitih područja.

Monitori su uređaju kod kojih se ovisno o potrebi TV nadzora koriste monitori određene veličine i svojstava razlučivanja detalja slike. Veličine monitora kreću se od 12.7 do 48 centimetara. Moć razlučivanja u centru monitora kreće se od 500 linija za

* Pinhole u prijevodu s engleskog znači mala rupica.

standardne monitore do 800 linija za monitore visoke rezolucije. Monitori u koloru imaju moć razlučivanja od 300 linija.

Uređaj za trajno snimanje slike (video-rekorderi) su uređaji kojima je osnovni zadatak da trajno registriraju sve događaje u alarmnom stanju, određenog dijela nadzornog sustava. Ručnim upravljanjem ili odgovarajućim programom automatski se odabiru pojedine mogućnosti. Standardne mogućnosti su izbor normalne brzine snimanja i brzine snimanja u alarmu. Time video-rekorderi mogu na jednu video - traku od 180 minuta snimiti 24 do 960 sati snimanja ovisno o odabranoj brzini, odnosno broju snimljenih slika u sekundi. Koliku brzinu snimanja ćemo odabrati ovisi o svrsi nadziranja, jer će kod velikog vremenskog perioda snimljenog na jednoj traci više informacija biti izgubljeno (na primjer, za 240 sati na jednoj traci slike se snimaju samo svake dvije sekunde, sve između toga je izgubljeno). Ovi video-rekorderi osim video ulaza mogu imati alarmne ulaze za primjenu brzine snimanja, alarmne izlaze, međusklop za daljinsko upravljanje rekorderom, mogućnost traženja alarma na video - traci, generator vremena i datuma itd.

Osim ovih video-rekordera postoje i takvi koji snimaju slike u realnom vremenu, ali samo alarmne događaje i to u trajanju od nekoliko sekundi do nekoliko minuta, ovisno o postavljenom vremenu snimanja.

Danas su sve više u upotrebi **digitalni rekorderi,** oni snimaju video slike na hard disk u digitalnom obliku. Na hard disk stane znatno više snimljenog materijala nego na video trake, a slike se mogu s hard diska presnimiti na neki magnetski medij (disketa, DAT, ZIP, CD) i prenijeti na računalo. Digitalni rekorderi najčešće imaju ugrađen multiplexer, pa je uz sve funkcije multiplexera moguće i snimanje svih kamera na hard disku uz mogućnost pojedinačnog pregledavanja te određivanja broja slika po kameri ovisno o aktivnostima u vidnom polju kamere ili alarma.

Kućišta i držači kamera su sastavni dio sustava TV nadzora na koje se ugrađuju kamere u najrazličitijim uvjetima. S obzirom na zahtjeve koji se postavljaju na pojedine kamere, kamere se ugrađuju s odgovarajućom dodatnom opremom koja osigurava zahtjevnu funkciju u prisutnim uvjetima okoline. Zato se kamere ugrađuju u posebna kućišta opremljena nekim od dodatnih uređaja: grijačima, ventilatorima, brisačima prozora kućišta, zaštitnim sjenilima itd. Ako su kamere pokretne, treba odabrati i odgovarajući model motoriziranog kućišta.

Preklopnici su uređaji koji nam omogućuju prikaz slika iz više kamera na jednom ili više monitora, a mogu biti ručni ili automatski. Preklopnici koji imaju

alarmne ulaze mogu u slučaju alarma prekidati slijedni prikaz i prijeći na stalan prikaz kamere u alarmu. Ako preklopnik ima više ulaza, možemo odrediti da na jednom monitoru gledamo slijed svih kamera, a na drugom samo odabranu kameru ili kameru u alarmu.

Multiplexer je uređaj koji omogućuje prihvaćanje video-signala s više kamera (na primjer 10) i istovremeno reprodukciju slika više kamera na jednom monitoru. Ovisno o modu koji je programiran moguće je prikazati istovremeno sliku svih 10 kamera.

Drugi modovi omogućuju prikaz određenog broja kamera na dijelu monitora, a na ostatku monitora prikazuje sliku jedne kamere.

Multiplexer nam omogućuje i zasebno namještanje osvjetljenja za svaku kameru. Multiplexeri mogu imati mogućnost upravljanja motorima za zakretanje kamere i zoom - objektiva, smrzavanje slike s mogućnosti povećanja, šifriranja tipkovnice za upravljanje multiplexerom itd.

Distributori su uređaji koji služe za djelovanje jednog video-signala u dva ili više pa se slike iz jedne kamere mogu promatrati na više mjesta.

Video-matrix sustavi su uređaji koji omogućavaju upravljanje velikim brojem kamera i monitora iz jednog nadzornog centra. Za velike sustave TV nadzora koriste se sustavi temeljeni na radu mikroprocesora, jedan takav sustav može prihvatiti na primjer 368 kamera i distribuirati signal na 32 monitora. Programira se koje kamere promatramo na kojem monitoru, posjeduju li alarmne ulaze i izlaze, te određuje na kojim monitorima se promatra slika u alarmu. Video-matrix sustavi mogu biti samostalni uređaji, ali su sve više u upotrebi sustavi bazirani na PC računalu. Ovi sustavi usklađuju rad i upravljanje svim računalima video sustava.

Quad kompresori su uređaji koji omogućavaju istovremeni prikaz slike iz četiri kamere na jednom monitoru, a svaka kamera zauzima 1/4 ekrana.

Video detektori kretanja su uređaji koji analizirajući video signal iz kamere pixel po pixel ili po zonama video signala i u slučaju promjene prema zadanom algoritmu određuju je li u vidnom polju kamere detektirano kretanje, te signaliziraju alarm. Prilikom odabira video detektora kretanja treba obratiti pažnju na rezoluciju, tj. broj pixela koji detektor analizira. Bolji detektori imaju mogućnost podjele video slike na dijelove koji se mogu uključiti ili isključiti iz analize tako da se na dijelu vidnog polja može događati kretanje bez aktiviranja alarma. Detektori za vanjsku upotrebu trebaju imati filtre za kompenzaciju promjene osvjetljenja scene i vremenske uvjete.

Općenito se video detektori instaliraju na kamere bez motora za zakretanje. Video detektori su veoma korisni kod 24 satnog nadzora jer je naporno konstantno gledati u monitor i tako nadzirati sustav. Video detektor će skrenuti pozornost stražarskom (zaštitarskom) osoblju na područje u kojem se detektiralo kretanje. Kod snimanja na video rekorder posebno se označava kada je u nekom području detektirano kretanje te će biti potrebno pregledati samo taj dio video trake.

Video detektori kretanja trebaju osigurati zaštitu prostora unutar i u blizini ograde. Sustav se sastoji od crno-bijelih kamera s objektivima fiksne žarišne duljine i IC reflektora koji osvjetljavaju prostor perimetra noću tako da je slika vidljiva za kamere i u slučaju da nestane vanjske rasvjete. Kamere se postavljaju na međusobnu udaljenost od 50 do 80 metara, prema konfiguraciji ograde i tehničkim zahtjevima sustava video detekcije. Sustav treba omogućiti detekciju neželjenih radnji (pokreta) u blizini ograde štićene zone. Karakteristike IC reflektora tipa FL-I/LED-60 W su: kut osvjetljavanja 20°, 50°, 80°, daljine osvjetljavanja 42, 55, 70 metara, napajanje od 100 do 230 V.

Sustavi prijenosa video-signala su:

1. Koaksijalnim kabelom.
2. Optičkim kabelom.
3. Putem parica.
4. Radio-prijenos.

1. **Koaksijalni kabel** je standardni medij, jeftin i jednostavan za instaliranje, te širokog područja propuštanja. Negativna strana je: potrebno je pojačalo ako kabel treba biti duži od 300 metara, osjetljiv je na elektromagnetske i radio-smetnje.
2. **Optički kabel** koristi modularni optički signal umjesto električkog signala. Može biti velike duljine, širokog je propusnog područja, male dimenzije i male težine, može se provoditi kroz eksplozivne sredine (ne koristiti električni signal), ne stvara radio-smetnje za okolne uređaje. Nedostatak optičkog kabela je u skupoći i složenom načinu spajanja.
3. Sustav prijenosa **putem parica** je jeftin jer se koriste jeftine neoklopljene ili oklopljene parice kao i za telefonske sustave. Za prijenos putem parica potreban je predajnik koji pojačava video-signal, te prijamnik. Nedostatak je potreba podešavanja da bi prijenos bio ispravan, te ograničeno područje propuštanja.
4. **Radio prijenos** omogućava bežični prijenos video signala u GHz frekvencijskom području. Prednost je pred žičanim u smanjenju cijene i vremena instaliranja,

jednostavnom premještanju, te stabilnosti rada. Nedostatak je u manje propusnom području i zahtjevu za čistim prostorom između predajnika i prijamnika. Veza može biti: **simplex** (prijenos samo u jednom smjeru), **duplex** (prijenos u oba smjera) i **multiplex** (više kanala prenosi se istim sustavom na različitim frekvencijama).

5. **Zahtjevi za rasvjetu,** rasvjeta vanjskog perimetra mora osigurati minimalnu razinu osvjetljenja 5 lux-a. Ukoliko to nije moguće ostvariti osnovnom, postojećom rasvjetom, potrebno je postaviti dodatna rasvjetna tijela koja će osigurati zahtijevanu vidljivost.
6. **Zahtjevi za napajanje,** primarno napajanje je 230 V/50 Hz. Zbog sigurnosnih razloga potrebno je predvidjeti alternativno napajanje svih uređaja. Alternativno napajanje mora osigurati autonomiju 24 sata. Na periferiji se mogu koristiti izvori napajanja iz pojedinih objekata, s osiguranjem alternativnog napajanja potrebnog kapaciteta, pri čemu izvori primarnog i alternativnog napajanja moraju biti osigurani od sabotaže.

3.4. Sustav kontrole pristupa

Pod kontrolom pristupa podrazumijevamo kontrolu i dozvolu pristupa i prolaza u štićeni prostor. Prostori koji su pod kontrolom prolaza i pristupa vozila i osoba, zaštićeni su vratima ili imaju barijere odgovarajuće čvrstoće i opremljeni su mehanizmima zatvaranja na koji se djeluje preko električnih veličina. Dozvola pristupa označava davanje naloga mehanizmu zatvaranja za njegovo otpuštanje. Za vrijeme trajanja naloga dozvole pristupa, omogućen je prolaz osobama koje su taj prolaz zahtijevale.

Dozvolu pristupa može ostvariti samo ovlaštena osoba koristeći se odgovarajućom **karticom, otiskom prsta "finger scan" ili kodom.** U kontrolnim jedinicama sustava, pojedinom kodu kartice pridružuju se svi podaci o posjedniku kartice i svi podaci koji definiraju status kartice odnosno imaoca kartice. Centralna kontrolna jedinica je računalo opremljeno perifernim jedinicama, programom i bazom podataka potrebnim za rad kontrolnog sustava. Kontrola pristupa može se ostvariti i bez kontakta.

Tehnički zahtjevi

Tehnički zahtjevi za djelovanje sustava kontrole pristupa su:

- Sustav i oprema moraju zadovoljiti zahtjeve ISO 9001.
- Sustav mora biti moduliran kako bi osigurao dogradnju sustava sukladno mogućim potrebama.
- Osigurati adekvatno osvjetljenje.
- Komunikaciju čitač – centar ostvariti preko optičkih kabela.
- Ovisno o tipu nosača koda udaljenost čitača može biti od 10 do 250 centimetara.
- Sustav mora imati alternativno napajanje za autonomiju 24 sata.

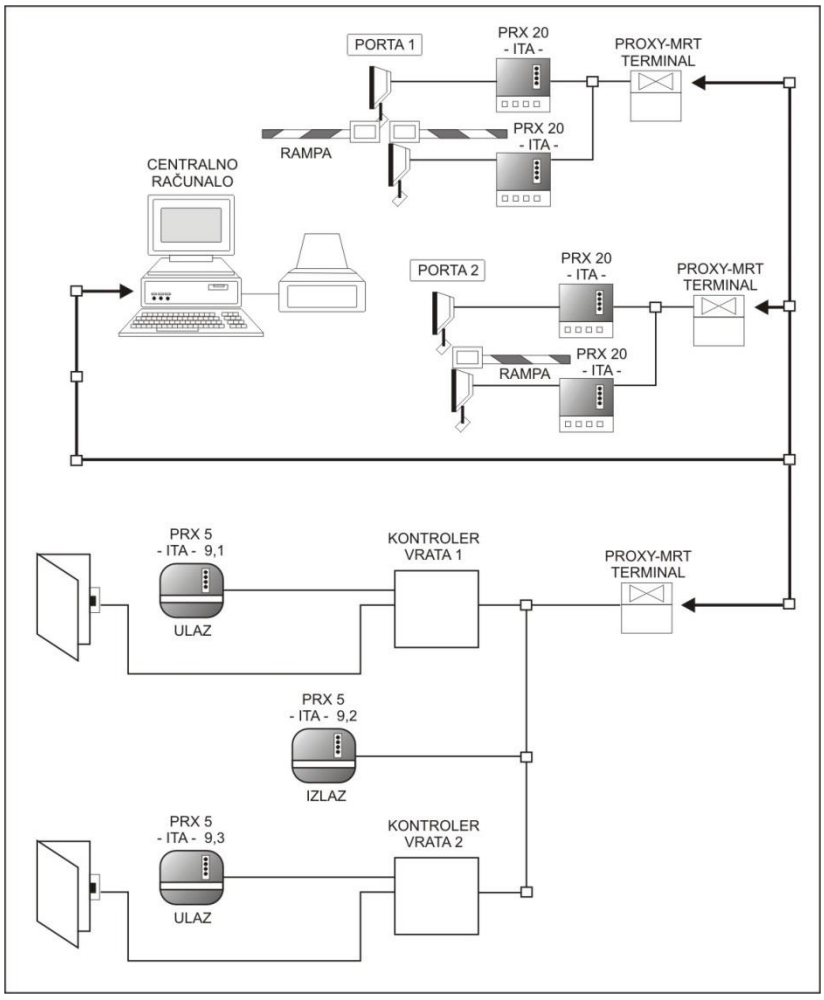
Funkcionalni zahtjevi

Funkcionalni zahtjevi za djelovanje sustava kontrole pristupa su:

- Sustav mora biti uporabljiv s PC računala.
- Sustav mora osigurati generiranje uputa osoblju stražarske službe u ovisnosti o vrsti alarmne situacije.
- Sustav mora tretirati odvojeno signal alarma, signal sabotaže i signal tehničke pogreške.
- Isključenje sustava može se ostvariti samo po propisnoj proceduri pomoću automatizacijskog koda.
- Sustav mora periodično komunicirati sa svim komponentama u svrhu provjere ispravnosti rada.
- Promjena napajanja s privremenog na alternativno ne smije izazvati alarm ali mora imati svjetlosno-zvučnu signalizaciju ispada privremenog napajanja.
- Jednim vratima moraju biti pridružena dva čitača, čime se omogućuje kontroliran ulaz i izlaz iz zaštićenog prostora.
- Vrata i brane, u kojima se ugrađuje uređaj za zatvaranje moraju odgovarati istoj razini sigurnosti.
- Vrata su načinjena za srednji mehanički stupanj zaštite.
- Vrata i brane jamče optimalnu funkcijsku sigurnost.
- Zapor i položaj vrata mogu se neprekidno nadzirati.
- Sustav mora biti kompatibilan sa svim elektroničkim sustavima kontrole pristupa.
- Računalo sustava mora automatski i trajno nadzirati pogonsko stanje, kao tijek funkcija te registrirati sve nepravilnosti.

Načelo djelovanja sustava

Beskontaktni sustav kontrole pristupa temelji se na elektroničkom nosaču koda koji obilježava osobe i vozila koji ga nose. Svaki nosač koda sadrži jedinstveno kodirani broj koji omogućuje pouzdanu identifikaciju. Podaci se od nosača koda beskontaktno individualnim putem prenose do čitača. Beskontaktni čitači su otporni na vandalizam, ne sadrže dijelove koji zahtijevaju održavanje ili zamjenu tokom korištenja. Treba samo prinijeti karticu čitača, čak i kada se ona nalazi u torbici ili novčaniku, vrata se otvaraju. Magnetsko polje prolazi kroz skoro sve materijale, pa se čitači mogu sakriti iza staklenih površina ili zida od cigle, a da još uvijek zadržavaju svojstva beskontaktnog čitanja (shema 7.).



Shema 7. Djelovanje sustava kontrole pristupa

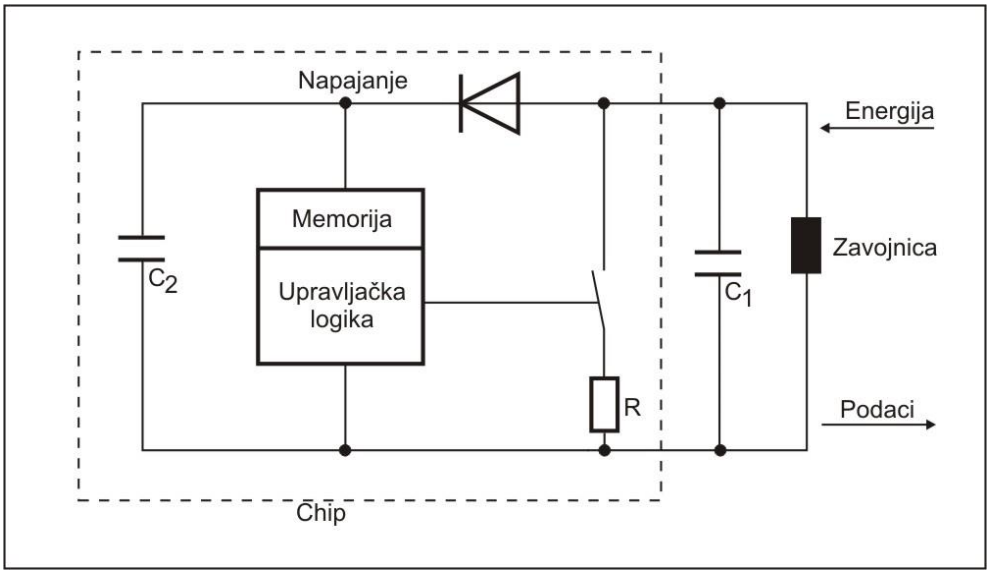
Tehničko rješenje sustava

Beskontaktni sustav kontrole pristupa sastoji se od sljedećih cjelina:

1. Nosača koda s jedinstveno kodiranim identifikacijskim brojem.
2. Čitača koji komuniciraju s nosačima koda i prenose podatke do terminala.
3. Terminala koji pohranjuje podatke, obavlja lokalna upravljanja, komunicira s ostalim terminalima i nadređenim centrom.
4. Jednog ili više centralnih računala koja omogućuju parametriranje terminala, generiranje izvještaja vezanih uz kontrolu pristupa ili registraciju radnog vremena, te komunikaciju s nadređenim procesnim sustavom.

1. **Nosači koda** (shema 8.) mogu biti u pasivnom ili aktivnom sustavu. **U pasivnom sustavu** nosači koda nemaju bateriju, zavojnica unutar čitača prenosi energiju do nosača koda i istovremeno služi kao prijamna antena za povratni signal. Očitavanje se ostvaruje na udaljenosti do 80 centimetara. Nosači koda su veličine kreditne kartice, pouzdani, jeftini i trajni, osnovna dva tipa nosača koda su: beskontaktna kartica i cilindrični nosač za montažu na vozila.

   U **aktivnom sustavu** nosači koda su napajani baterijom koja se nalazi u nosaču, izmjena baterije je jednostavna i može je obaviti korisnik. Očitavanje se ostvaruje na udaljenosti do 250 centimetara, a programiranje nosača koda obično obavlja proizvođač.



Shema 8. Blok dijagram nosača koda

2. **Beskontaktni čitači** sastoje se od:
   - RF dijela
   - mikroprocesorskog dijela
   - optičke i akustičke signalizacije korisniku
   - komunikacijskog dijela.

a) **RF dio** napaja energijom nosač koda generiranjem elektromagnetskog polja.

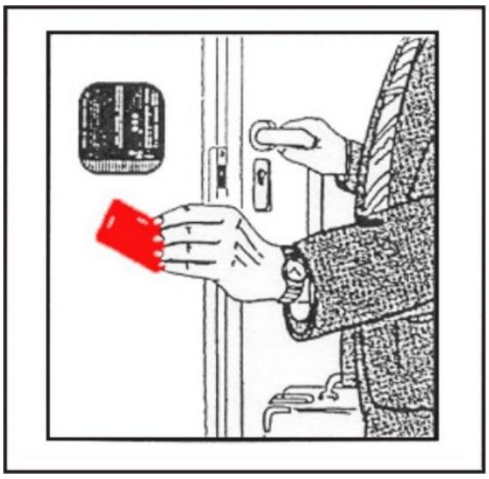
b) **Mikroprocesorski dio čitača** prihvaća demodulirani signal, dekodira ga, te samo ako je ispravno primljen prenosi ga komunikacijom do terminala.

c) **Optička i akustička signalizacija korisnika** – čitač se obično montira u blizini vrata ili neke druge fizičke barijere, van štićenog prostora, čitač je opremljen s 3 svjetlosna LED indikatora i zvučnikom.

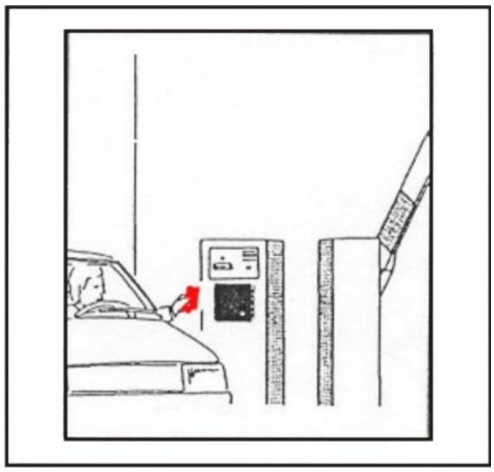
d) **Komunikacijski dio** – u trenutku kada se uspravan nosač koda nađe u blizini čitača, žuta LED indikacija i zvučnik signaliziraju prisutnost nosača koda, podatak se prenosi do terminala koji aktiviranjem crvene ili zelene LED indikacije može signalizirati dozvolu pristupa u štićeni prostor za posjednika nosača koda.

U **pasivnom sustavu** postoje tri tipa čitača:

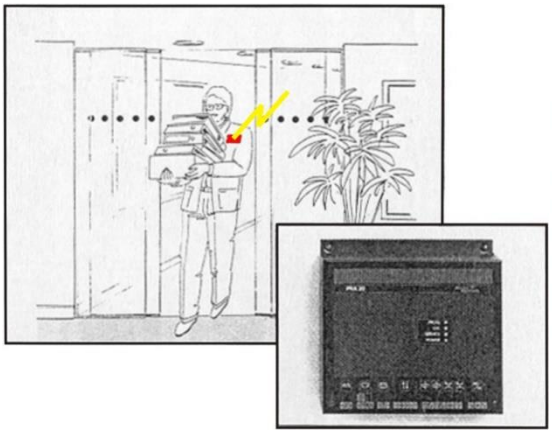
1. Udaljenost čitanja je od 5 do 8 centimetara, koristi se za kontrolu pristupa i registraciju radnog vremena (slika 12).
2. Udaljenost čitanja je do 20 centimetara, koristi se za identifikaciju vozila (slika 13.).
3. Udaljenost čitanja je do 80 centimetara, koristi se za kontrolu pristupa s *"hands free"* karakteristikama, diskretnost instalacije (slika 14.) i sustav identifikacije vozila (slika 15.).



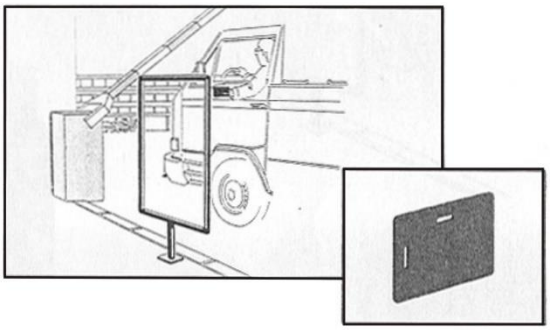
Slika 12.



Slika 13.

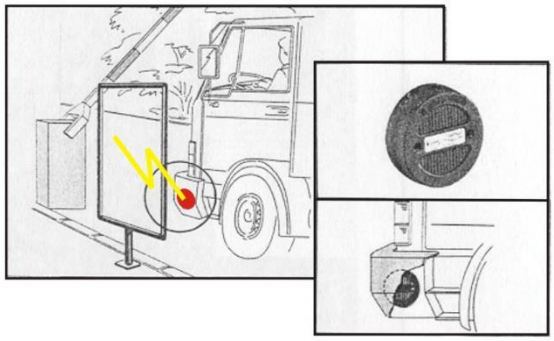


Slika 14.



Slika 15.

U **aktivnom sustavu** koji se koristi za identifikaciju vozila, udaljenost čitanja ovih čitača je do 250 centimetara (slika 16.).



Slika 16.

3. **Terminali** pohranjuju informacije koje su pročitane s nosača koda, do prenošenja na centralno računalo. Terminali obavljaju upravljanje stanjem vrata aktiviranjem električne brave, u slučaju da pristup nije dopušten upravljanje vratima se ne obavlja, dok se pokušaj pristupa u štićeni prostor memorira. Terminali posjeduju komunikacijski dio s kojim ostvaruju vezu s centralnim računalom, te prijenos informacija o prisustvu nosača koda na pojedinim mjestima do centralnog računala.
4. **Centralna računala** su PC kompatibilna računala, ona omogućuju parametriranje terminala, prihvaćanje podataka s terminala, generiranje izvještaja, te komunikaciju s uređenim procesnim sustavom, te određuje koji nosači koda imaju dozvolu pristupa i u koje određeno vrijeme. Na osnovu podataka prikupljenih s terminala na centralnom računalu moguće je generirati izvještaje vezane uz kontrolu pristupa kao što su:
   - svi prolazi kroz određena vrata u nekom periodu

- prolazi određenog nosača koda u nekom periodu
- vrijeme koje je djelatna osoba ili stražar proveo na poslu itd.

3.5. Sredstva veze

Za stražarske službe (zaštitarske) od izuzetnog je značaja imati dobru, brzu i kvalitetnu vezu između nadzornog centra i stražara (zaštitara), te stražara međusobno na štićenom objektu ili površini. Veza se uspostavlja na različite načine, na primjer **javnom telekomunikacijom** (mobitel,), **radijskom vezom** (fiksna, mobilna, prijenosna) koriste se uređaji kao što su: RADIUS P210 – Motorola, RU 12, **žičana veza** koja se ostvaruje induktorskim telefonima, telefonskim središnjicama (induktorski telefon M-63) itd.

Tehnički zahtjevi

Od sredstava veze koja se koriste najzastupljenija je radijska veza “Motorola RADIUS P210” i žičana veza “induktorski telefon M-63”, od kojih se zahtijeva:

1. Radius P210 – motorola

- Frekvencijski opseg: VHF (136-174 MHz), UHF (403-520 MHz).
- Broj kanala: 8 ili 16.
- Razmak kanala: 12.5 kHz i 20/25 kHz.
- RF izlazna snaga: 2 – 5 W (VHF), 2 – 4 W (UHF).
- NF izlazna snaga: 500 mW.
- NF frekvencijski opseg: 300 – 300 Hz (+1 – 3 dB).
- Osjetljivost: 20 dB (0,34 nV).
- Izvori energije: NiCd akumulator (10V/1000 mAh), duljina rada 9 – 13 sati.
- Doseg: simpleksna veza (u opsegu do 2 km), dupleksna veza/REPETITOR (više stotina kilometara).

2. Induktorski telefon M-63

- Veza može biti ostvarena neposredno između dva telefona ili preko centrale.
- Po kabelu PBK-2 veza se ostvaruje do 30 km, a po stalnim zračnim linijama do 150 km.

- Impedancija: 6 Ω.
- Izvor električne energije: dvije baterije R-20 od 1,5 V.

Funkcionalni zahtjevi

Funkcionalni zahtjevi za djelovanje sredstava veze su:

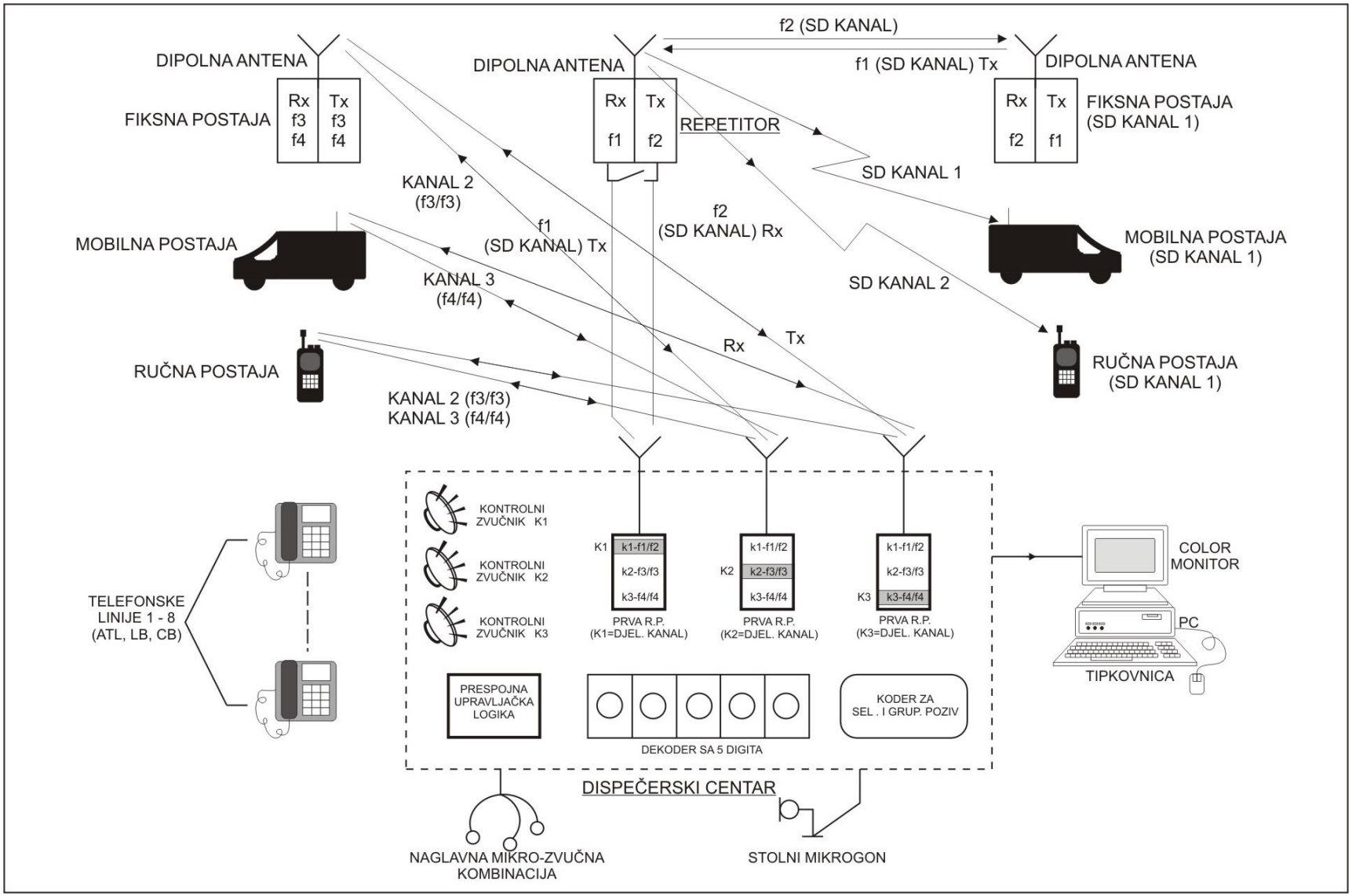
- Moramo imati dobru, brzu i kvalitetnu radijsku vezu između nadzornog centra i stražara te stražara međusobno na objektu (području) koji se štiti.
- Moramo osigurati tajnost informacija koje se prenose, a posebno tajnosti informacija koje se prenose u izvanrednim situacijama.
- U radio sustavu treba osigurati da prednost prenošenja informacija imaju stražari koji će se naći u izvanrednoj situaciji.
- Nije dopušteno zlorabiti pravo prednosti ako to određena situacija ne zahtijeva.
- Vlasnik radio sustava ne smije ometati rad drugih sustava veza.
- Nije dopušteno slati lažne znakove opasnosti.
- Na radio-postaji se mogu primati samo one frekvencije za koje je namijenjen taj sustav.
- Za učinkovitu radio-komunikaciju u zaštitarskoj službi potrebno je razraditi sustav komuniciranja koji će biti prilagođen uvjetima rada stražarske službe.
- Za pouzdani sustav dojave potrebno je upoznati sve sudionike u vezi s načinom komuniciranja (sporazumijevanje može biti djelomično i šifrirano).
- Pri sporazumijevanju razgovori su kratki.
- Operater u nadzornom centru (centrali) poziva stacionarne i mobilne postaje te obavlja provjeru stanja.

Načelo djelovanja

Cilj svakog sustava komuniciranja je ostvariti brz, jednostavan i pouzdan sustav veza. Veza se može ostvariti (vidi shemu 9.) na sljedeće načine:

1. Nadzorni centar (centrala) zove stacionarnu ili mobilnu postaju.
2. Stacionarne i mobilne postaje zovu nadzorni centar (centralu).
3. Stacionarna postaja zove mobilne i ostale stacionarne postaje.
4. Prijenosna postaja zove stacionarnu.
5. Sistem selektivnog pozivanja i identifikacije.

1. **Nadzorni centar (centrala) zove stacionarnu ili mobilnu postaju.** Veza se ostvaruje između operatera u nadzornom centru (centrali) i stacionarne ili mobilne postaje, pozivom kodnog broja stanice s kojom se želi uspostaviti veza. Osim selektivnog poziva, operater na centrali može ostvariti i grupnu vezu.
2. **Stacionarne i mobilne postaje zovu nadzorni centar (centralu),** postupak je isti kao i u prethodnom slučaju.



Shema 9. Organizacijska shema vanjskog sustava UKV veza s dispečerskim centrom (20)

3. **Stacionarna postaja zove mobilne i ostale stacionarne postaje,** postupak je isti samo se veza između svih stanica ostvaruje preko repetitora, a repetitor ima zadaću da primljeni signal od stanice pojača i proslijedi dalje.
4. **Prijenosna postaja zove stacionarnu,** mreža je otvorena bez uređaja selektivnog i grupnog poziva. Stražar, kada je kanal slobodan, upućuje tonski poziv i u stacionarnoj stanici se izbacuje identifikacijski broj. Operater najavljuje stanicu i preuzima poruku, a poslani identifikacijski broj je dekodiran i ispisan na indikatoru.
5. **Sustav selektivnog pozivanja i identifikacije** može biti:
   - jednotonski
   - dvotonski
   - tonsekventni.

   Selektivno pozivanje ima mogućnost optičke i akustičke signalizacije poziva i vrlo često se ugrađuje posebno u ručne (prijenosne) radijske postaje. Sustav za identifikaciju se sastoji od:
   - prijamnika selektivnog poziva
   - dekodera znamenki
   - pokazivača brojeva.

   On se nalazi na pultu nadzornog centra, gdje operater, na svjetlosnom pokazivaču vidi identifikacijski broj mobilne ili fiksne postaje, te zna s kim razgovara, prednosti tog sustava su:
   - velika disciplina u mreži
   - bolja informiranost
   - brža razmjena poruka
   - veća sigurnost u radu.

Tehničko rješenje sustava veze

Radijski sustav NKV veza sastoji se od: radijskih postaja (repetitora, fiksnih, mobilnih i prijenosnih postaja) s pripadajućim instalacijama (antene). Nadzorni centar se sastoji od:

1. Radijskog dijela.
2. Telefonskog dijela.
3. Kompjutorskog dijela.

1. **Radijski dio** ima koder za selektivni, grupni i prioritetni poziv, operater biranjem selektivnog, a potom identifikacijskog broja (kojeg imaju ugrađene ručne prijenosne postaje) stupa s njima u vezu (na prvom, drugom ili trećem kanalu). Dolaskom ID broja on se dekodira na dekoderu u nadzornom centru, tako da se odmah zna tko je zvao.

2. **Telefonski dio** je skup elektronskih sklopova koji omogućuju spajanje 1 – 8 telefonskih (ATC, LB i CB) linija na nadzorni centar, osim toga omogućuje "ulaz" s određene telefonske linije na bilo koju radijsku postaju na terenu (fiksnu, mobilnu, prijenosnu) i obrnuto.
3. **Kompjutorski dio** putem PC uspostavlja se radijskom i telefonskom mrežom preko tipkovnice.

3.6. Nadzorni centar

Zahtjevi za nadzorni centar sukladno Pravilniku o uvjetima i načinu provedbe tehničke zaštite (N.N. 198/03) su: omogućiti učinkovitu zaštitu štićenog objekta kroz stalni nadzor nad štićenim objektom s jednog mjesta, centralni prijam i signalizaciju alarma, provedbu plana postupanja u izvanrednim slučajevima, rekonstrukciju događaja, odnosno okolnosti koje su prethodile nastupanju izvanrednog slučaja, nadzor nad radom i budnosti osoblja zaduženog za sigurnost objekta i provedbe propisanog radnog režima na objektu, te zaštita povjerljivih podataka i informacija od poslovnog i drugog interesa koji su pohranjeni u računalima.

Tehnički zahtjevi

Tehnički zahtjevi za djelovanje nadzornog centra su:

- Mora se osigurati primarno i alternativno napajanje za sve uređaje u nadzornom centru za autonomiju 24 sata.
- Svi uređaji osim sučelja za rad osoblja (monitori, tipkovnica idr.) moraju biti predviđeni za *rack* ugradnju u ormare.
- Ormari za smještaj opreme moraju biti opremljeni ventilacijom i klimatizacijom radi smanjenja utjecaja dicipacije energije.
- Ormari moraju biti postavljeni i/ili izrađeni tako da osiguravaju pristup kabliranju i uređajima sa stražarske strane u svrhu održavanja, postavljanja ili popravka.
- Nadzorno-zapovjedni pult mora biti projektiran i izrađen tako da osigura preglednost i brz i jednostavan dostup u svrhu izdavanja zapovijedi.
- Prostor nadzornog centra mora imati sljedeće sadržaje i opremu:
  - prostorija nadzornog centra
  - čajna kuhinja
  - sanitarni čvor
  - prostorija za odmor s ležajem i internom svjetlosno-zvučnom signalizacijom
  - klima-uređaj.

- Svi navedeni prostori moraju biti odijeljeni sigurnosnim sustavom kontrole prolaza od ostalog dijela objekta u koji se centar smješta.
- Centar se ne smije nalaziti u blizini vanjske ograde.
- Svi prozori moraju biti ojačani rešetkom i neprobojni za metak.

Funkcionalni zahtjevi

U nadzornom centru, osim već spomenutih funkcionalnih zahtjeva u poglavlju 6.5., potrebno je osigurati:

- prihvat svih signala s pojedinih uređaja na periferiji
- automatsko i ručno upravljanje izdavanjem zapovijedi
- interaktivni grafički prikaz
- internu svjetlosno-zvučnu signalizaciju prorade
- statističku obradu podataka.

Načelo djelovanja

Sustavi međusobno razmjenjuju informacije preko centralne opreme za obradu signala u nadzornom centru, (shema 10.), iz nje je vidljivo načelo djelovanja tj. upravljanje i nadzor nad drugim sustavima sa svrhom osiguranja odgovarajuće razine sigurnosti, kao i moguća uporaba sustava tehničke zaštite u druge svrhe npr. protupožarna zaštita itd.

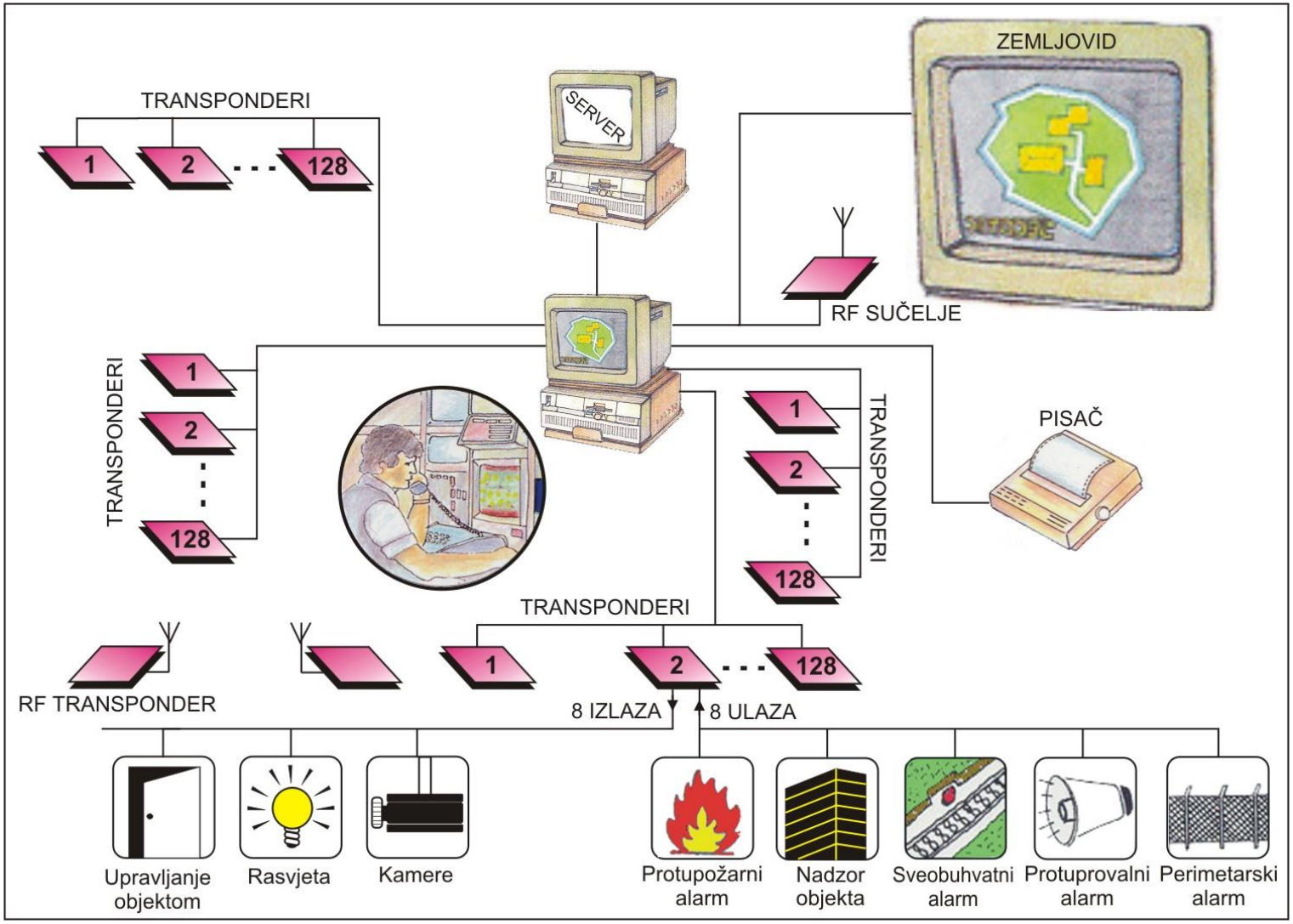
Tehničko rješenje nadzornog centra

Nadzorni centar mora biti spreman na perimetru sveobuhvatno riješiti, odnosno nadzirati i upravljati sa:

- zaštitnom ogradom
- sustavom video-nadzora
- sustavom protuprovale
- sustavom kontrole pristupa osoba i vozila
- sustavom kontrole zaštitarske ili stražarske službe, odnosno sredstava veze koja koriste.

Glavni elementi nadzornog centra su:

- računalo
- kolor monitor
- štampač
- besprekidno napajanje
- komplet opreme za komunikaciju
- programska potpora.



Shema 10. Djelovanje nadzornog centra

Tehničko rješenje nadzornog centra integriranih sustava zaštite složenih objekata, kao što su: vojni objekti, objekti za preradu opasnih tvari, temelji se na prostorno distribuiranom, računalom upravljanom nadzorno – upravljačkom sustavu. Ovakvim rješenjem sustava zaštite, funkcije prethodno navedenih sustava povezane su u jedinstvenu cjelinu.

Pomoću dislociranih modula prikupljaju se informacije o stanju detektora u perimetru te se te informacije preko dvožilne komunikacije prenose u centar. Iz centra se preko ovih modula upravlja s ulazom u vojarnu, skladišta, baze i sl., rasvjetom, alarmima itd. Preko operatorske konzole u nadzornoj sobi, omogućuje se nadzor i upravljanje radom sustava od samo jednog operatera.

1. **Nadzor** preko PC-a i digitaliziranog grafičkog prikaza zaštite perimetra, moguće je imati brzu i preciznu informaciju o stanju detektora. U slučaju alarma na ekranu se prikazuje mapa alarmirane zone, aktivira se zvučni signal, ispisuje se operateru uputstvo za rad u slučaju dotičnog alarma. Operater potom može na ekranu pogledati detaljnije upute za rad u slučaju dotičnog alarma, pogledati uputstva za rad u slučaju izvanrednog događaja (provale, sabotaže itd.) pogledati uvećanu mapu područja iz kojeg je primljen signal alarma.
2. **Upravljanje** prilikom alarma automatski se obavi zadana sekvenca aktiviranja pojedinih izlaza, pale se svjetla, šalje se poruka video - sustavu za uključenje odgovarajuće kamere ili video-rekordera, itd. Pored toga moguće je i ručno postaviti neke izlaze iz grupe ili grupu izlaza (upaliti svjetla, aktivirati određenu zvučnu ili svjetlosnu signalizaciju, itd.). Nakon što je otklonjen uzrok alarma operater resetira dotični alarm, pri čemu se također odvije automatska sekvenca upravljanja.
3. **Arhiviranje i obrada liste alarma i liste događaja** prilikom alarma ispisuje se alarmna poruka na štampač i automatski se sprema informacija o dotičnom alarmu u arhivu računala. Svi događaji i sve akcije operatera bilježe se u memoriji računala, što omogućuje naknadnu rekonstrukciju događaja pregledavanjem liste događaja, pri tom je moguće dobiti kronološki pregled liste alarma, pregled sortiran po broju ulaza, pregled sortiran po broju zone ili pregled svih dnevnih aktivnosti na sustavu.

4. **Automatska i ručna promjena stanja nadzora nad detektorima i zonama** moguće je ručno pojedini detektor ili grupu detektora, zonu ili grupu zona, transporter ili grupu transportera, te sve zone odjednom postaviti u neaktivno ili sigurnosno stanje. Na taj se način može npr. privremeno deaktivirati zona u kojoj se očekuje dopuštena aktivnost koja bi inače prouzročila alarm. Osim ručnim nalogom, moguće je ovakve manipulacije obaviti i automatski po unaprijed zadanom vremenskom programu, na taj je način moguće programirano razlikovati ponašanje sustava zaštite u različitim periodima dana.
5. **Kreiranje prikaza i funkcija sustava,** ovaj sustav također omogućuje kreiranje ili primjenu grafičkih mapa, promjenu konfiguracije sustava (broja ulaza ili izlaza, rasporeda zona, veze ulaza s pojedinom zonom, itd.), zadavanje sekvenci automatskog upravljanja, itd.
6. **Autorizacija aktivnosti operatera,** sve aktivnosti nad sustavom operatera moraju biti autorizirane šifrom. Za razne korisnike postoje različite razine ovlaštenja čime se postiže da npr. smjenski poslužilac ne može izbrisati listu događaja, neautorizirano mijenjati konfiguraciju sustava ili uputstva za slučaj ekscesa itd. Naravno, autoriziranoj osobi ove su funkcije dopuštene.

3.7. Zahtjevi za rasvjetu

Rasvjeta vanjskog perimetra mora osigurati minimalno razinu osvjetljenja 5 luksa. Ukoliko to nije moguće ostvariti osnovnom, postojećom rasvjetom, potrebno je postaviti dodatna rasvjetna tijela koja će osigurati zahtijevanu vidljivost.

U unutrašnjosti objekta, u prostoru gdje je predviđen sustav video nadzora mora se osigurati rasvjeta razine osvjetljenja 15 luksa.

3.8. Zahtjevi za napajanje

Primarno napajanje je 230 V/50 Hz. Zbog sigurnosnih razloga potrebno je predvidjeti alternativno napajanje svih uređaja, alternativno napajanje mora osigurati autonomiju 24 sata.

Na periferiji se mogu koristiti izvori napajanja iz pojedinih objekata, s osiguranjem alternativnog napajanja potrebnog kapaciteta, pri čemu izvori primarnog i alternativnog napajanja moraju biti osigurani od sabotaže.

4. NAJZNAČAJNIJI SIGURNOSNI SUSTAVI U AUTOMOBILIMA

U vrijeme kada je osobno vozilo postalo potreba a ne luksuz, gotovo je nemoguće zamisliti da isto nije opremljen raznim sustavima sigurnosti. Pored aktivnih sustava postoje i pasivni sigurnosni sustavi koji služe zaštiti putnika u vozilu od ozljeđivanja, odnosno smanjenju opasnosti od ozljeđivanja prilikom sudara vozila. Kako bi se omogućila potpuna sigurnost putnika u vozilu, takvi sustavi se moraju međusobno nadopunjavati. Tako sigurnosni zračni jastuci i sigurnosno vjetrobransko staklo gotovo da i nemaju nikakvog smisla ako putnik u trenutku prometne nesreće nije vezan. Za razvoj sigurnosnih sustava u cestovnom prometu zadužene su razne neovisne organizacije koje umjetno izazovu prometnu nesreću kako bi izvršile testiranje raznih sigurnosnih sustava. NCAP je jedna od njih, a djeluje na području nekoliko kontinenata.

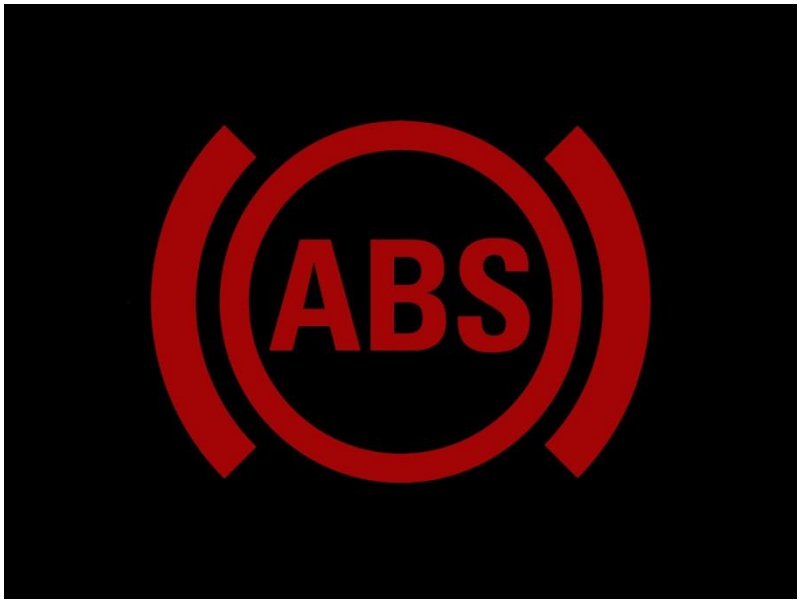
4.1. ABS i ESP sustavi

Slika 17. Testiranje na bočni udar

Strelovit napredak aktivnih i pasivnih sigurnosnih sustava u automobilima rezultirao je osjetno manjim brojem nesreća, pogotovo onih s fatalnim posljedicama. Ipak, već letimičan pogled na crnu kroniku bilo kojeg dnevnog lista

otkriva da se tragične nesreće događaju svakodnevno. Razlog većine je neprilagođena brzina, a nerijetko kumuje i prekomjerna doza alkohola.
U proteklih 10 godina na hrvatskim cestama poginulo je 174 djece, a gotovo 15.000 ih je ozlijeđeno. To je dovoljan razlog da još jednom napomenemo kako su svi ovdje navedeni sustavi isključivo od pomoći vozaču, ali ne mogu kompenzirati neodgovorno ponašanje.
Automobili su sigurniji nego ikad prije, a za nekoliko desetljeća prometne nesreće postat će stvar prošlosti. Većina novih modela osvaja maksimalnih pet zvjezdica na testovima sigurnosti, ESP je postao obavezan za sve nove automobile na tržištu EU, sve više se vodi računa o sigurnosti pješaka i djece te umoru vozača, razvijeni su zračni jastuci za putnike straga, autonomna vozila testiraju se u realnim uvjetima…

4.2. ABS sustav



Slika 18. Oznaka ABS sustava

Sustav za sprječavanje blokiranja kotača tijekom kočenja korijene vuče iz avijacije. Patentirao ga je Gabriel Voisin još 1929., a pamtimo i uspješan Dunlopov sustav Maxaret iz 50-ih. Automobilsku je premijeru doživio u Jensenu FF 1966., a Chrysler, Ford, Nissan i General Motors počeli su ga nuditi početkom 70-ih. Širu

popularnost stekao je nakon što je dorađen Boschov sustav 1978. ugrađen u najveće modele Mercedesa i BMW-a, a od 1994. je obavezan u svim novim automobilima. ABS (eng. Anti-lock braking system) zapravo je elektroničko-hidraulički mehanizam koji, sprječavanjem blokiranja kotača, omogućava skraćivanje zaustavnog puta te promjenu smjera vožnje prilikom naglog kočenja. Na mekanim podlogama poput makadama i pijeska, iznimno, može produžiti zaustavni put, ali, obzirom na brojne prednosti, to je zanemarivo. Sustavi novije generacije kontroliraju i raspodjelu kočenja između prednjih i stražnjih kotača te time izvlače maksimum iz kočnog sustava. Svojim djelovanjem smanjuje vjerojatnost prometne nezgode za čak 18 posto.

4.3. ESP sustav

Slika 19. Prikaz djelovanja ESP sustava

Ključan sustav aktivne sigurnosti korijene vuče iz 1987. Upravljačka elektronika, na temelju brzine, bočnog ubrzanja i brzine vrtnje vozila oko vertikalne osi prepoznaje zanošenje te pulsirajućim kočenjem pojedinih kotača i smanjenjem snage motora, vraća automobil na putanju, bez utjecaja vozača. Obvezan je od studenoga 2014.

4.4. Airbag sustav

Slika 20. Prikaz djelovanja airbeg sustava

Konstruirao ga je John W. Hetrick 1952., Chrysler je počeo s ugradnjom 1967., a prvi europski model bio je Mercedes-Benz S-klase (W126) iz 1980. Nekoliko milisekundi nakon sudara, upravljački modul aktivira kapsulu sa 8 g eksploziva. Izgaranjem se oslobađa dušik koji puni jastuk, nakon amortizacije udarca se prazni, a ciklus traje 150 ms.

4.5. Laminirano staklo

Slika 21. Laminirano staklo nakon udara

Izumio ga je 1903. Édouard Bénédictus, francuski kemičar, a već 1911. primjenjuju ga u automobilima. Britanska vlada uvela je zakonsku obvezu 1930., nakon što su istraživanja pokazala kako smanjuje rizik od ozljeda. Najčešća izvedba sastoji se od dva sloja stakla debljine 2,5 mm između kojih je sigurnosna folija debela 0,38 mm.

4.6. Sigurnosni pojas

Slika 22. Pojas s pričvršćenjem u tri točke

Pojas s pričvršćenjem u tri točke stvorio je 1959. Nils Bohlin, a prvi pokušaji sežu u 1885. kad je Edward J. Claghorn patentirao pojas u dvije točke. Korištenjem pojasa putnici izbjegavaju nagle trzajne pokrete i udarce u armaturu. Brojni protivnici smatrali su da ugradnjom pojasa kupcima poručuju da su njihovi automobili nesigurni. Država Victoria u Australiji prva je uvela zakonsku obvezu korištenja 1970.

4.7. Crash testovi

Slika 23. Testiranje vozila na sudare

Sigurnost automobila napreduje svjetlosnom brzinom, a konačan cilj razvoja aktivnih i pasivnih sigurnosnih sustava je promet s nula nesreća (Vizija 0). Nažalost, neopreznim i neodgovornim vozačima nema pomoći, jer granice fizike i zdravog razuma ne može pomaknuti ni sva sila elektronike.

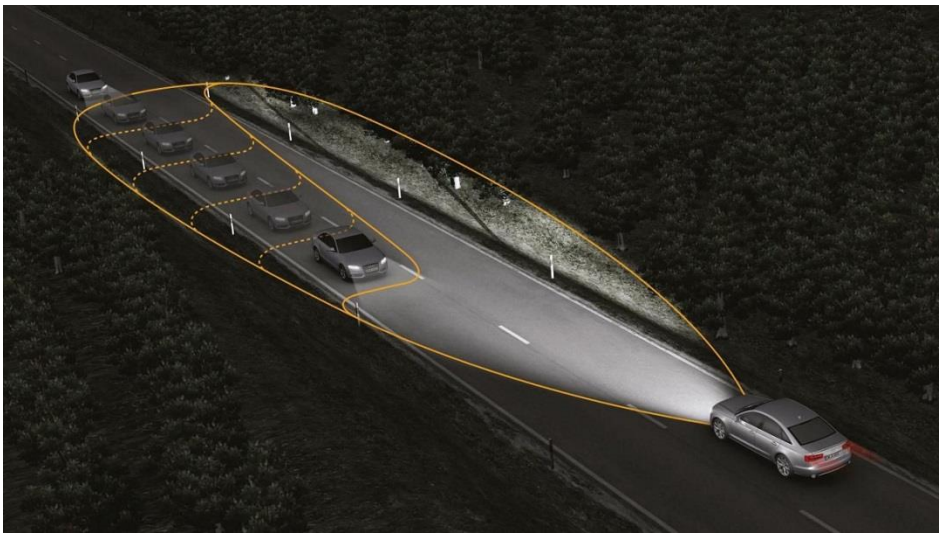
Danas se sigurnost automobila uspoređuje rezultatima s EuroNCAP testiranja. Prve crash testove u povijesti provodio je GM, još davne 1934., a Mercedes je 1949. redovito zabijao model 170 u fiksnu prepreku kako bi istražili djelovanje sile udara na konstrukciju.

4.8. EBD I BAS sustavi

Slika 24. Sustav EBD

Sustav EBD ovisno o brzini vozila i trenju između gume i podloge elektronički raspodjeljuje snagu kočenja za svaki kotač posebno, dok sustav BAS pojačava snagu kočenja ovisno o brzini reakcije na papučicu kočnice. Inauguriran je 1996. u Mercedes-Benzu S-klase nakon što su istraživanja pokazala kako 90 posto vozača, zbog neiskustva i šoka, u kritičnoj situaciji ne pritisnu papučicu potrebnom silom.

4.9. Adaptivna svjetla



Slika 25. Adaptivna svjetla

Senzori stalno bilježe brzinu vozila, kut skretanja i zakreta upravljača, detektiraju objekte pored ceste, pješake i nadolazeća vozila, pa značajno bolje osvjetljavaju cestu.

4.10. Deformacijske zone

Slika 26. **Deformacijske zone -** preduvjet za crash-test

Nakon pogibije Ayrtona Senne 1994. u Imoli masovno su se počele koristiti deformacijske zone. Već 1936. Citroën je ispitao otpornost na oštećenja Traction Avanta obrušivši ga niz liticu, kako bi se vidjelo koliko je siguran. Sustavne crash-testove Mercedes provodi od 1953., kad je predstavljen model 180 (W120). Po principu akcije i reakcije sva nakupljena kinetička energija mora se negdje distribuirati. Primjerice, automobil mase dvije tone pri 60 km/h udarit će u nepomičnu prepreku silom kao da je bačen s visine od 14,2 m, a pri 90 km/h ekvivalentna visina je 32 m, odnosno 50% veća brzina povećava silu udara za 125%.

Slika 27. Mrtvi kut

Sustav za detekciju vozila u mrtvom kutu (BLIS - Blind Spot Information System), premijerno ugrađen u Volvo S80 2007., radarskom detekcijom provjerava stanje, prilikom pretjecanja ili promjene vozne trake, te potom svjetlosnim i zvučnim signalima upozorava vozača na moguću opasnost.

4.11. LDW sustav

Slika 28. LDW sustav na kontrolnoj ploči

Sustav Lane Departure Warning, koji je razvio Nissan 2001., kamerom te infracrvenim ili radarskim senzorom prati oznake na cesti te zvučnim i svjetlosnim signalima upozorava vozača ako nesvjesno krene izlaziti iz prometne trake. Nova generacija (Toyota 2004.) samostalno korigira putanju.

4.12. Stražnji zračni jastuci

Slika 29. Prikaz djelovanja stražnjih zračnih jastuka

Autonomna vozila nisu više samo vizija budućnosti. Kad stignu u masovnu upotrebu broj nesreća drastično će se smanjiti, ali pojavit će se drugi problemi, poput hakerskog napada na softver automobila ili infrastrukture.

Stražnji jastuci stižu 2017., a obveza će postati već od 2022. Opsežna njemačka studija GIDAS (German In-Depth Accident Study) pokazala je da više od 50 posto teških i fatalnih ozljeda putnika na stražnjim sjedalima dolazi uslijed udara glave o naslon prednjih sjedala ili djelovanjem prevelike reakcijske sile pojasa, izazvane inercijskom silom tijela pri naglom usporenju u sudaru, te posljedičnih ozljeda prsnog koša i vitalnih organa. To je posebno važno, jer se na stražnjim sjedalima često voze djeca i stare osobe, koji su izložene povećanim rizicima teških i smrtonosnih ozljeda. Paralelno se razvijaju koncepcije zračnih jastuka koji se napuhuju iz krova i onih koji se napuhuju iz poleđina naslona prednjih sjedala. Tvrtka TRW Automotive Holdings Corp. razvila je i usavršila drugi sustav, koji omogućuje bolji prihvat tijela i 'mekšu' amortizaciju. Mana je što se mijenja razmak između stražnjeg naslona i putnika na stražnjim sjedalima, ovisno o uzdužnom položaju sjedala te nagibu naslona. Budući je teško pronaći optimum, stručnjaci

TWR-a razvijaju sustav promjenjive brzine i tlaka napuhivanja na temelju ta dva parametra, koja se prate senzorima. Zbog toga se podjednak naglasak daje i na razvoj krovnog zračnog jastuka.

4.13. TPMS sustav

Slika 30. TPMS sustav na kontrolnoj ploči

Sustav Tire Pressure Monitoring System sastoji je od niza senzora integriranih u kotače koji putem bežične veze (radiosignala) šalju informacije o tlaku i temperaturi svake gume. U slučaju brzog gubitka tlaka vozača na problem upozorava signalna lampica na armaturi. Premijerno je ugrađen u Porsche 959 1986.

4.14. Prekid dotoka goriva

Slika 31. Ventili za prekid dotoka goriva

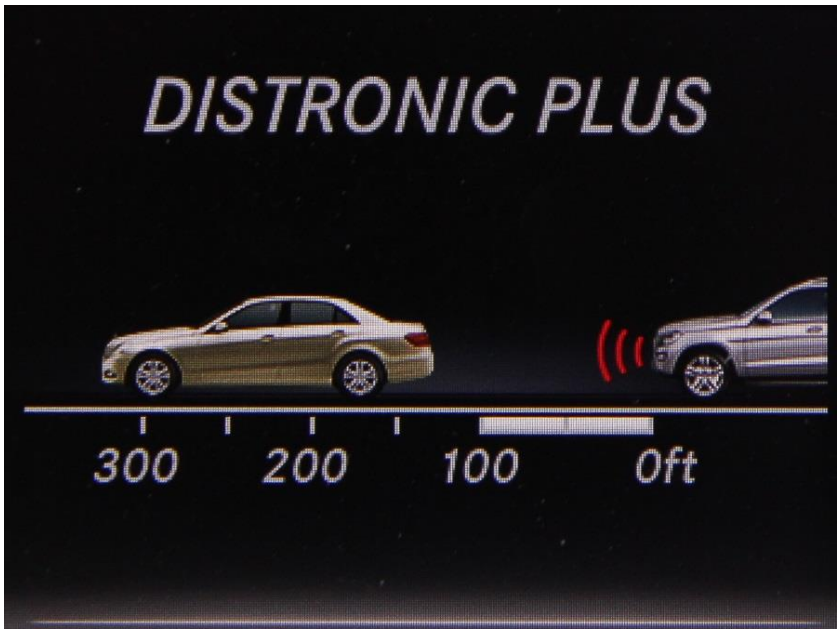
Već nekoliko milisekundi nakon što ECU registrira signal o aktivaciji zračnih jastuka zatvara se ventil na izlazu iz pumpe goriva te prekida napajanje strujom sustava za ubrizgavanje goriva. Time se umanjuje mogućnost pojave požara nakon sudara, a gorivo zajedno s parama ostaje na sigurnom - u spremniku.

4.15. Autonomno kočenje

Slika 32. Sustav autonomnog kočenja

Razmjerno novi sustav (uveo ga je Volvo 2010.) zasad nije u širokoj primjeni, a procjenjuje se da će, kad postane obvezan, smanjiti broj sudara za čak 27 posto. Set senzora sprijeda (kamera, laser i radar) detektira nailazak na vozilo ili prepreku koje se kreće znatno nižom brzinom. U trenutku kada procijeni da je krajnje vrijeme za početak kočenja, a u nedostatku reakcije vozača, sam zaustavi automobil.

4.16. Aktivni tempomat



Slika 33. Djelovanje tempomata

Prvi aktivni tempomat temeljen na laserskoj tehnologiji uveo je Mitsubishi 1995. Vozaču je dovoljno samo unijeti željenu udaljenost od vozila ispred, a sustav će samostalno taj razmak održavati, zahvaljujući podacima iz lasera u prednjem braniku. Ako se iznenada smanji, upozorit će ga zvučnim i svjetlosnim signalima.

4.17. HUD sustav

Slika 34. Prozirni ekran HUD sustava

Tehnologija čiji je razvoj počeo za potrebe vojnog zrakoplovstva pred početak II. Svjetskog rata, primjenu je našla i u automobilima (GM 1988.). Premda Head-Up Display izgleda kao projekcija, zapravo je riječ o prozirnom ekranu na kojem se prikazuju važni podaci o vožnji, vidljivi bez skretanja pogleda sa ceste.

5. ZAKLJUČAK

Briga za sigurnost svim živim bićima prirođena je kao instinkt, kojoj je čovjek dodao još skup svjesnih postupaka i ponašanja, a koji proizlaze iz činjenice da rizici nisu nametnuti čovjeku kao pojedincu, niti društvu u cjelini već su dio njegove naravi, njegova života.

Porastom stupnjeva, načina i modela ugrožavanja “prirodnog” u suvremenoj civilizaciji raste i broj načina, sredstava, metoda, tehnika i sl. kojima se opasnosti i posljedice rizika mogu otkloniti ili barem smanjiti na onu podnošljivu mjeru koja se podnošljivom smatra u danom socijalnom kontekstu. Na taj se način razvija “nova normalnost” (5).

Proučavanjem opasnosti i rizika polazimo od pretpostavke da rizik i opasnosti postoje kao objektivne činjenice čije se postojanje može ustvrditi, procijeniti i poduzeti mjere da se njihovo negativno djelovanje umanji ili u potpunosti isključi.

Neupitna je činjenica da je današnje društvo "društvo rizika". U svijetu postoje bezbrojne ugroženosti i opasnosti koje su usmjerene prema svim, posebno temeljnim vrijednostima ovoga svijeta koje se mogu podijeliti u četiri skupine (12):

- Čovjek – njegov život i zdravlje, njegova prava i slobode i njegova ostvarenja.
- Ljudsko društvo, međunarodni poredak, konkretna (globalna) društva, države,...
- Materijalna dobra.
- Ekosustav.

Ova problematika neiscrpan je izvor za proučavanje različitih znanosti kao što su: društvene, političke, vojne.

Kojim je sve rizicima i opasnostima koje donosi tehnološki napredak, koje donosi suvremeno društvo rizika, izložen čovjek, odgovorili smo u poglavlju, osnovni oblici ugrožavanja osoba i imovine.

Pored propisa kojima je regulirana zaštita osoba i imovine, osiguravajuća društva razvila su i razvijaju osiguranje čovjeka i imovine kao jednu od tehnika za upravljanje rizicima za rizike koje je moguće osigurati. Osiguranje se razvilo iz potrebe da se rizik kojemu su izloženi pojedinci pravilno rasporedi na sve osiguranike. Zadaća osiguravajućih društava je da na osnovu plaćenih premija osiguranja "preuzimaju" rizik za pokriće određenih šteta.

Zaštitarske tvrtke u suradnji s osiguravajućim društvima, suvremenom elektroničkom i informatičkom industrijom, sigurnosnim službama i drugima, razvile su i razvijaju sredstva, naprave i uređaje koji intergrirani čine sustave tehničke zaštite kako bi se opasnosti i rizici otklonili ili smanjili na najmanju moguću mjeru.

Procjena ugroženosti i analiza prikupljenih podataka izrađena je primjenom priznatih pravila u provedbi tehničke zaštite. U nedostatku hrvatskih normi primijenjene su odgovarajuće europske norme (EN, IEC, ISO) te prihvaćena pravila struke.

Tehnička zaštita predstavlja skup radnji kojima se neposredno ili posredno zaštićuju ljudi i njihova imovina, a provodi se tehničkim sredstvima i napravama te sustavima tehničke zaštite kojima je osnovna namjena spriječavanje protupravnih radnji usmjerenih prema štićenim osobama ili imovini[*]. Sustavi tehničke zaštite predstavljaju, povezivanje dvaju ili više sredstava, naprava i uređaja koji zajedno čine funkcionalnu cjelinu.

U vrijeme kada je osobno vozilo postalo potreba a ne luksuz, gotovo je nemoguće zamisliti da isto nije opremljen raznim sustavima sigurnosti.
Sigurnost vozila može se promatrati kroz aktivnu i pasivnu sigurnost. Aktivni elementi „ pomažu“ vozaču pri upravljanju vozilom, pokušavaju „natjerati“ vozilo da se ponaša kako to vozač želi. Pasivni elementi su „posljednja linija obrane“. Oni pomaţu da putnici u vozilu
zadobiju što manje i što bezazlenije ozljede u trenutku kad nastupi prometna nesreća.
Kako se ovi elementi ponašaju u stvarnosti, ispitiva se različitim testiranjima. Pri tome su posebno interesantna ispitivanja pasivne sigurnosti koja se provode pomoću tzv. crash testova pri čemu se simuliraju različiti oblici prometnih nesreća.

[*] Pravilnik o uvjetima i načinima provedbe tehničke zaštite (N.N. broj 198/03).

6. LITERATURA

[1] Appelt, H.: Video-nadzor, Jutarnji list, VI, 2003, 1685, str. 50-51.
[2] Brzezinski, Z.: Izvan kontrole, Zagreb, Otvoreno sveučilište, 1994.
[3] Čaldarović, O.: Društvo i rizici, Zagreb, IPROZ, 2002.
[4] Čaldarović, O., Nehajev Rogić ,J., Subašić, D.: Kako živjeti s tehničkim rizikom. - Zagreb: APO, 1997.
[5] Čaldarović, O.: Socijalna teorija i hazardni život, Zagreb, 1995.
[6] Čolović, D.: Video-nadzor ispred 17 škola i 15 vrtiča, Jutarnji list, VI, 2004, 2057, str. 15.
[7] Duspara, M.: Osiguranje političara, Nacional, 23, 2003, 419, str. 26.
[8] Graphic News: Sud pravde sudi o izraelskom zidu, Nacional, 24, 2004, 432, str. 9.
[9] Hungtington, P.S.: Sukob civilizacija. - Zagreb, Izvori, 1998.
[10] Hrvatski ceh zaštitara: Preporuke hrvatskog ceha zaštitara, HCZ-0401. – Zagreb: Studio Žiljak d.o.o., 2004.
[11] Ivanjek, Ž.: Bijes koji je podijelio svijet i nije kaznio krivce, Jutarnji list, V, 2002, 1539, str. 50-51.
[12] Javorović, B.: Sigurnost – Hrvatska i svijet, Mjere i sredstva za zaštitu od terorizma, Zagreb, IPROZ, 2001, str. 5-9.
[13] Kričanić, M.: Zaštita automobila s aspekta Zakona o zaštiti osoba i imovine, Svijet osiguranja, IV, 2001, 2, str. 29.
[14] Miljuš, D.: Tema broja, Večernji list, 47, 2003, 14400, str. 8-9.
[15] Peić, K.: Video-nadzor za odvračanje pljačkaša, INA glasnik, XLI, 2004, 1822, str. 13.
[16] Rudeš, T.: Znanost i terorizam, Jutarnji list, VI, 2003, 1718, str. 15.
[17] Skupina autora: Priručnik za stručno obrazovanje radnika unutrašnjih poslova. - Zagreb, MUP RH, 1990.
[18] Skupina autora: Priručnik za izobrazbu čuvara, Zagreb, LAS, 1997.
[19] Toma, I.: Opasnost za Hrvatsku mafia i terorizam, Jutarnji list, VI, 2003, 1872, str. 3.
[20] Vaughan, E.J. i Vaughan, T.M.: Osnove osiguranja, Upravljanje rizicima, Zagreb, Mate d.o.o., 2000.
[21] Vujević, M.: Uvod u znanstveni rad, Zagreb, Školska knjiga, 2000.
[22] https://autoportal.hr/clanak/najznacajniji_sigurnosni_sustavi_u_automobilima