

ALARMNI SISTEMI

Predavanje 12

Zaštita od provale – opšti zahtevi

Bezbednost objekata i prostora – osnovne mere:

građevinsko - urbanističke mere

građevinsko - arhitektonske karakteristike objekta, uređenje okolnog prostora, funkcionalnost pojedinih celina i bezbednosni zahtevi,

organizacione mere

organizacija službe obezbeđenja, raspoređivanje njenih pripadnika, usavršavanje, itd.,

operativne mere

organizacija prikupljanja informacija, nadzor nad prostorom koji se štiti i primena represivnih postupaka i mera, kao i mera koje su bitne bezbednost objekata i prostora koji se štiti, i

tehničke mere

primena sredstava i uređaja za otkrivanje, identifikaciju i signalizaciju neželjenih događaja.

Zaštita od provale – opšti zahtevi

Faktori koji direktno određuju veličinu i karakteristike sistema za zaštitu od provale i prateće službe obezbeđenja:

- makro i mikrolokacija objekta,
- vrsta i vrednost sadržaja u objektu,
- svakodnevne aktivnosti, organizacija rada u objektu, tehnološki proces u objektu (ako postoji),
- mogućnosti i oblici komunikacije i kretanja u prostoru oko objekta i u samom objektu, itd.

Faktori na kojima se zasniva funkcionisanje sistema bezbednosti:

- procena ugroženosti,
- projekat sistema tehničke zaštite,
- organizovana služba obezbeđenja i
- plan obezbeđenja.



Nadzor okoline

Nadzor spoljašnjeg dela objekta

Nadzor u unutrašnjosti objekta

Nadgledanje predmeta (cilja ulaza)

Nečujno alarmiranje

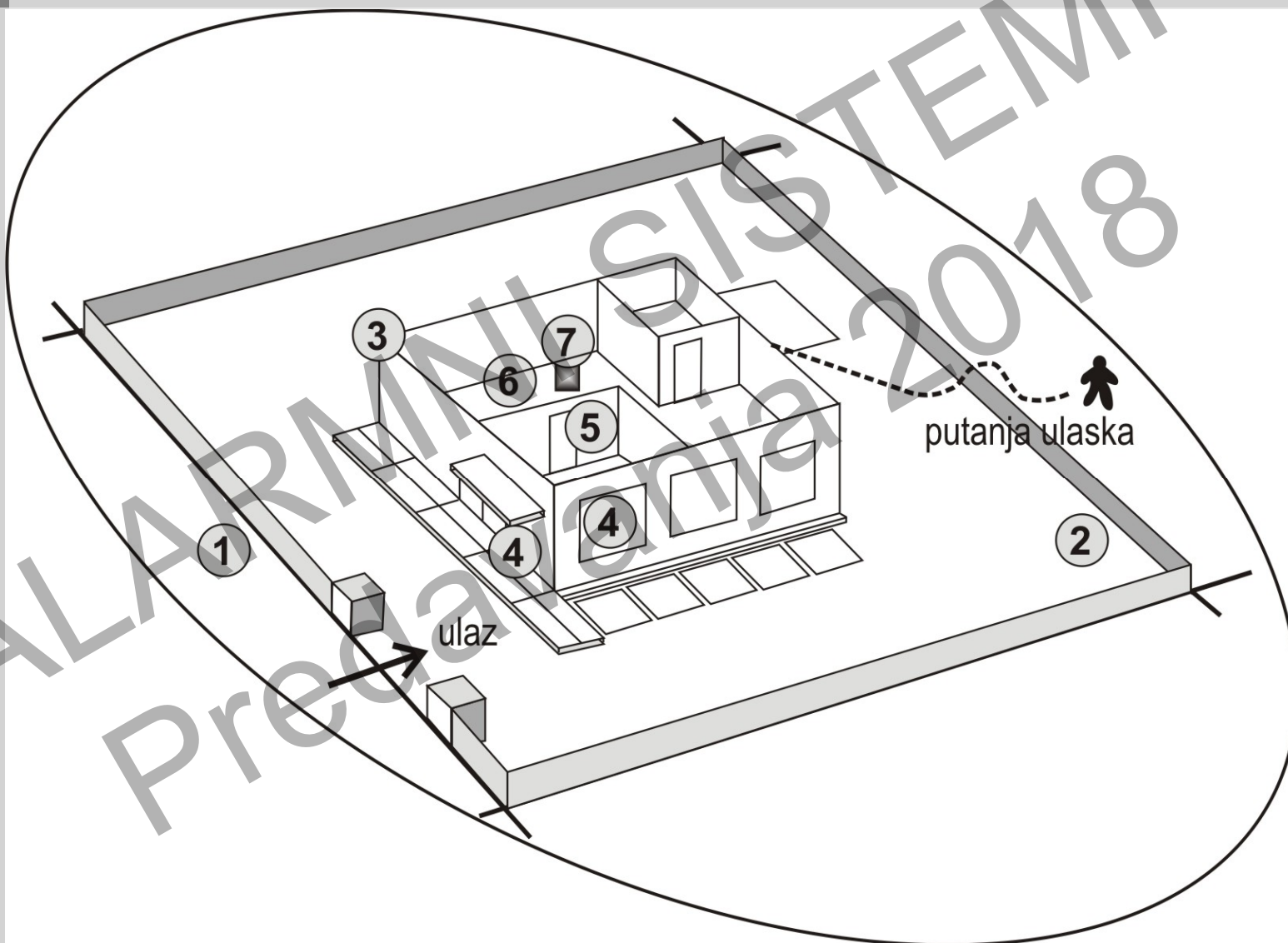
Organizacija zaštite od provale

Grupe mera za otkrivanje ulaska u prostor koji se štiti:

1. *mere kojima se otkriva neželjeni ulaz u prostor ili u objekat,*
2. *mere kojima posle ulaska lica otkriva kretanje u prostoru ili objektu i*
3. *mere kojima se vrši legitimisanje ili identifikacija lica.*

Sedam odbrambenih „prstenova“ (linija odbrane) – **“ZLATNI BROJ 7”**:

1. linija perimetra (sa ili bez fizičkih barijera),
2. prostor između perimetra i objekata u kompleksu,
3. granica objekta (zidovi),
4. otvori na objektu (vrata, prozori, razni otvori),
5. unutrašnje pregrade,
6. neposredna okolina cilja,
7. cilj - razlog neovlašćenog ulaska (krajnja tačka prilaza).



Organizacija zaštite od provale – nivoi zaštite

Definicija nivoa zaštite u odnosu na efekte odvrćanja i sprećavanja

Nivo 1 - minimalna zaštita. Najniži nivo zaštite i u materijalnom pogledu. Neovlašćeni pristup se sprećava fizićkim barijerama, ogradama, vratima i prozorima od standardnog materijala i sa obićnim bravama. Ovo je najćešći nivo zaštite koji se primenjuje kod stambenih zgrada i na javnim objektima.

Nivo 2 - nizak nivo zaštite. Prvi nivo zaštite sa jednostavnim alarmnim sistemima, sa ili bez komunikacije sa višim nivoom nadzora (policija, službe obezbeđenja). Najćešće se primenjuje u privatnim kućama, manjim trgovinama, ekspoziturama banaka, itd.

Nivo 3 - srednji nivo zaštite. Jednostavniji alarmni sistemi - detekcija neovlašćenog pristupa na perimetru i delimićno u unutrašnjosti zone koja se štiti + postojanje službe fizićkog obezbeđenja. Najćešće primenjuje kod zaštite banaka, muzeja, velikih trgovina i slićno.

Nivo 4 - visok nivo zaštite. Sprećavanje, otkrivanje i procena neovlašćenog pristupa na liniji perimetra, u unutrašnjem prostoru i u samim objektima. Sve što ima nivo 3 + sistem za kontrolu pristupa (identifikacione kartice, sistem biometrije i sl.), sistem zatvorenog video nadzora (CCTV) i dobro organizovana služba fizićkog obezbeđenja. Primenjuje za zaštitu objekata od velikog znaćaja - materijalnog, društvenog, proizvodnog, itd.

Nivo 5 - maksimalna zaštita. Kompletna zaštita spolja i unutra primenom svih komponenti koje ima nivo ćetiri, sistem je deo integrisanog sistema. Najređi u praksi i primenjuje se kod kompleksa koji su od posebnog stratećkog i društvenog znaćaja.

Karakteristike sistema za zaštitu od provale

Tri najznačajnije karakteristike sistema:

- *verovatnoća detekcije,*
- *stopa lažnih alarmiranja i*
- *„osetljivost“ sistema na pokušaje obilaženja ili izbegavanja detektora.*

Verovatnoća (pouzdanost) detekcije zavisi od:

1. količine i karakteristike emitovane energije,
2. veličine objekta,
3. rastojanja od objekta,
4. brzine objekta,
5. pravca kretanja,
6. karakteristike refleksije /apsorpcije energije od strane „uljeza“ i okruženja.

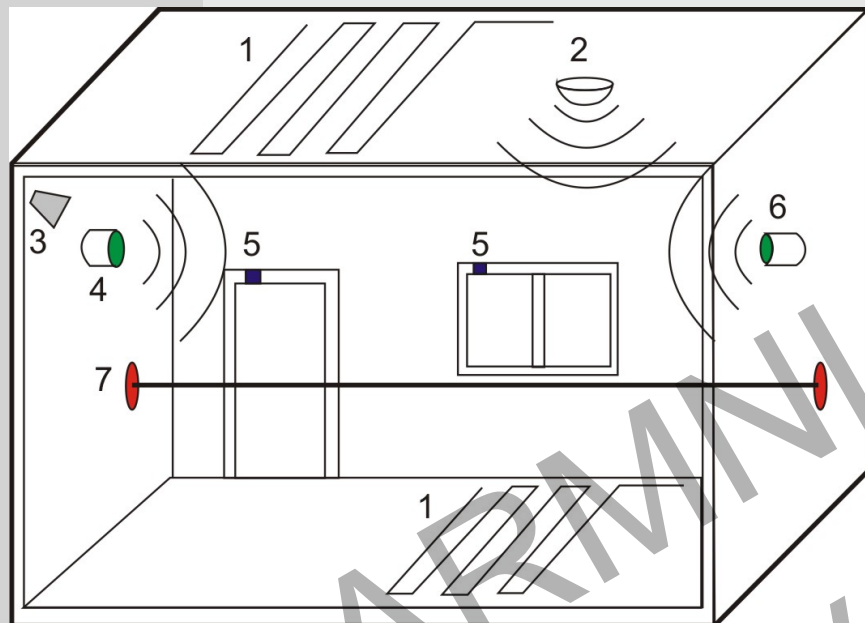
Lažna alarmiranja:

1. **Smetnje** - tip lažnog alarma čije poreklo je donekle ili potpuno poznato (kretanje životinja, EM smetnje),
2. **Lažni alarmi** - ne zna se poreklo, inicijalno se shvataju kao stvarni alarm, ali se kasnije proveraju.

“Osetljivost” sistema:

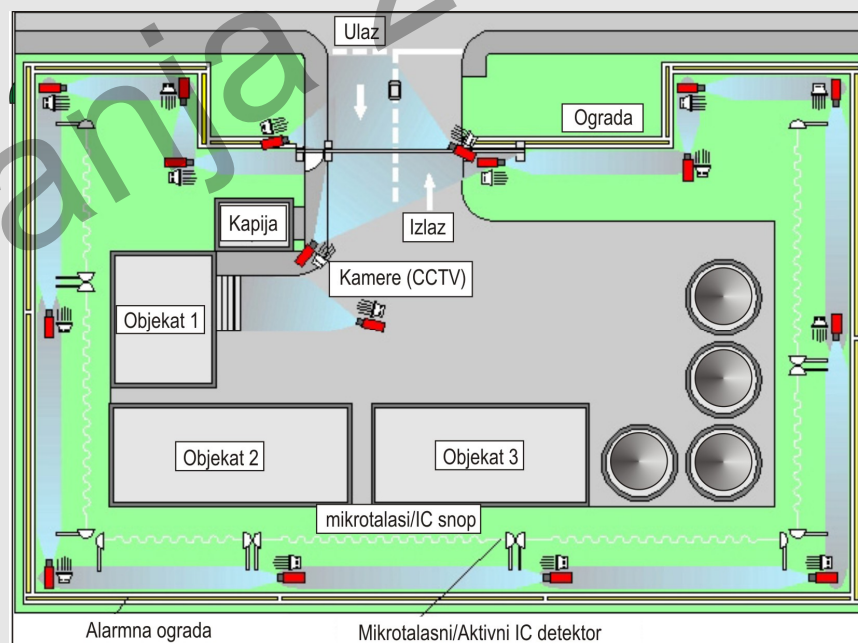
Izbegavanje zona pokrivanja različitim načinima ulaska. Slabe tačke“ sistema se obezbeđuju:

- pokrivanjem sa više detektora istog tipa i/ili više detektora različitog tipa,
- preklapanjem zona detekcije i
- međusobnom zaštitom detektora od onesposobljavanja.



Primer spoljašnje zaštite od provale ->

<- Primer unutrašnje zaštite od provale

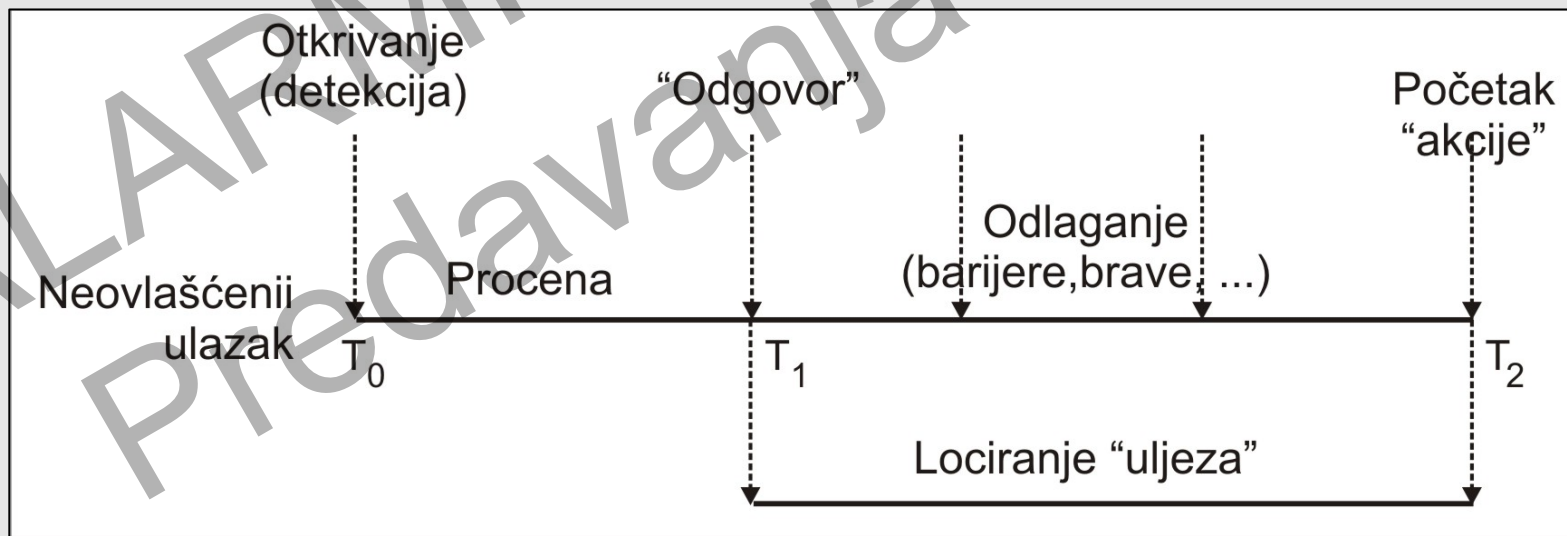


Projektovanje sistema za zaštitu od provale

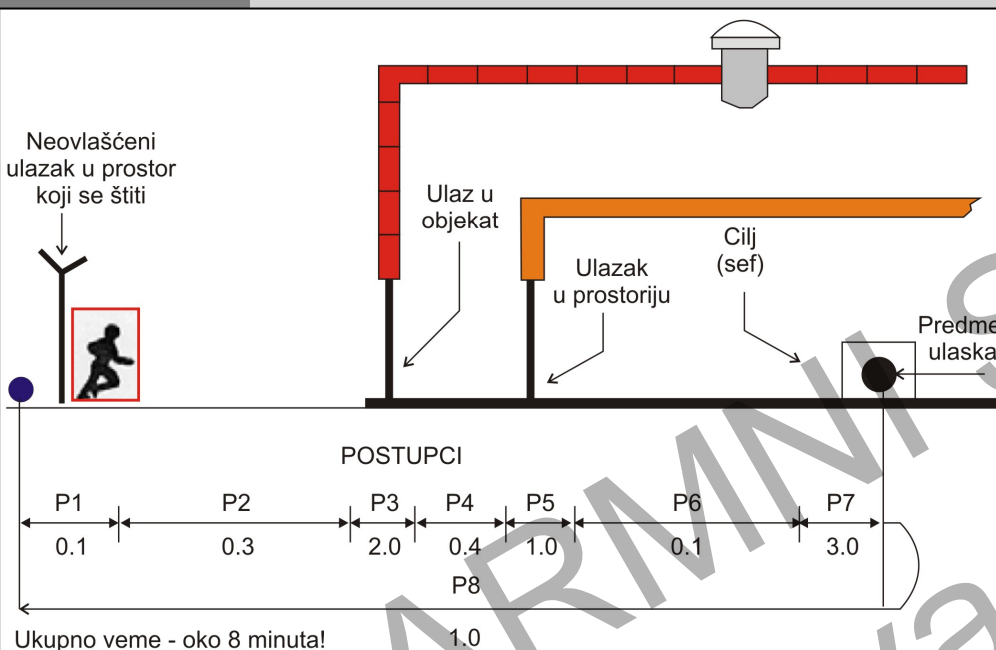
Tri faze realizacije zaštite od provale (*detect - delay - respond*):

1. **detekcija** neovlašćenog ulaska u prostor/objekta,
2. vreme od upada do dolaska do cilja u objektu (**kašnjenje**),
3. **odgovor/akcija** službe fizičkog obezbeđenja.

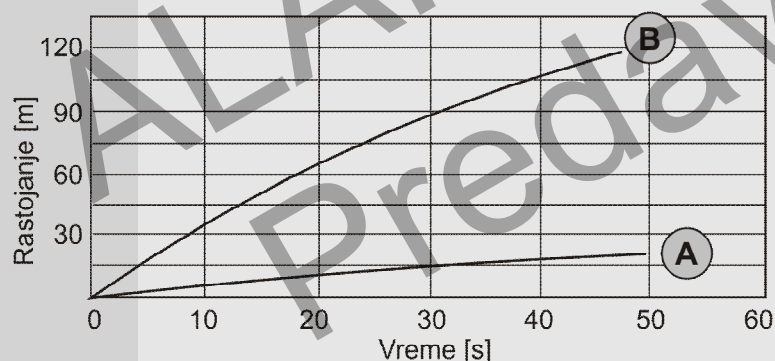
“Scenario” neovlašćenog ulaska:



Projektovanje sistema za zaštitu od provale



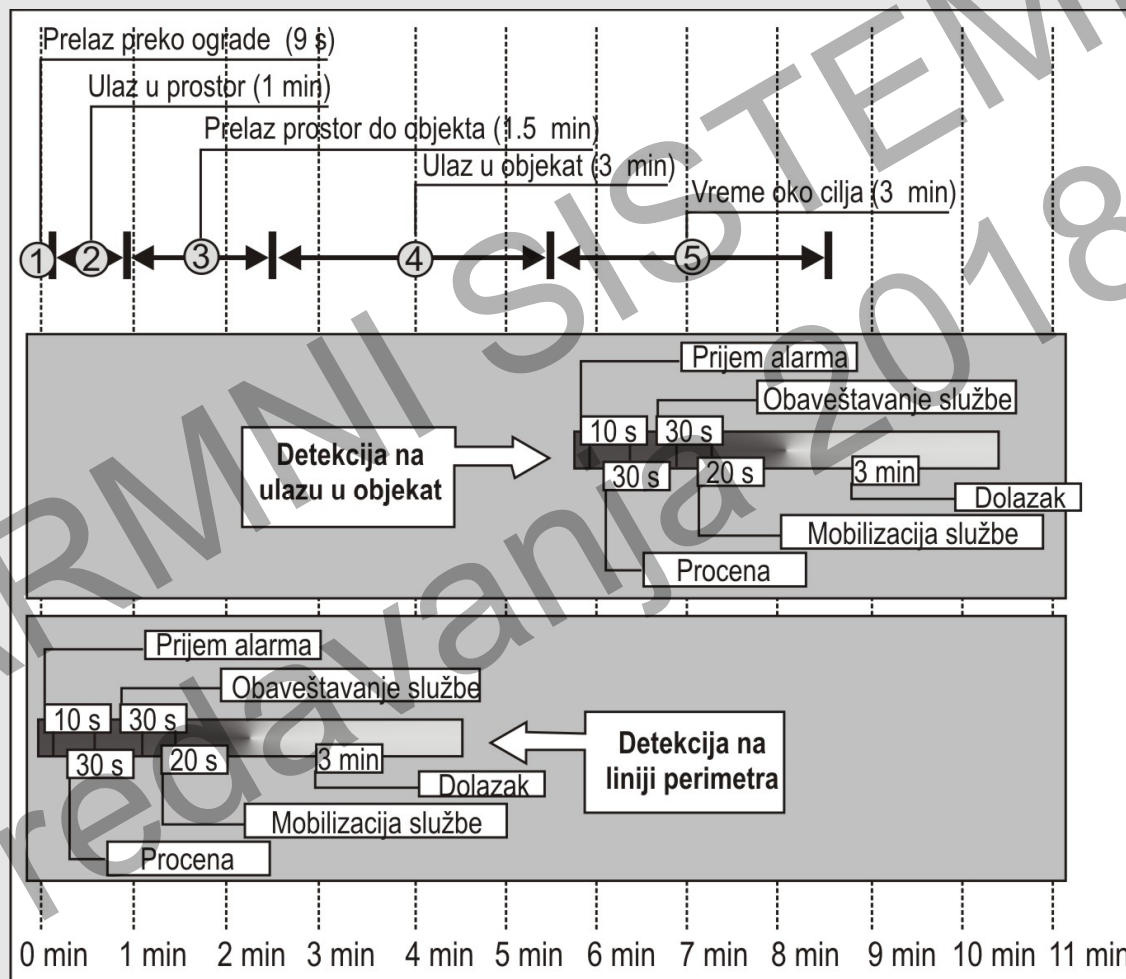
Postupak	Vreme (min)	Opis
P1	0.1	Prelazak ograde
P2	0.3	Pretrčavanje 75 m
P3	2.0	Prolazak kroz vrata
P4	0.4	Prelazak 16 m
P5	1.0	Obijanje brave
P6	0.1	Dolazak do cilja
P7	3.0	Otvaranje sefa
P8	1.0	Uzimanje materijala i bekstvo
Ukupno	7.9	Ukupno vreme boravka



Kretanje sa teretom (alat težine 16 kg): **kriva A: penjanje uz stepenice, kriva B: trčanje na otvorenom prostoru**

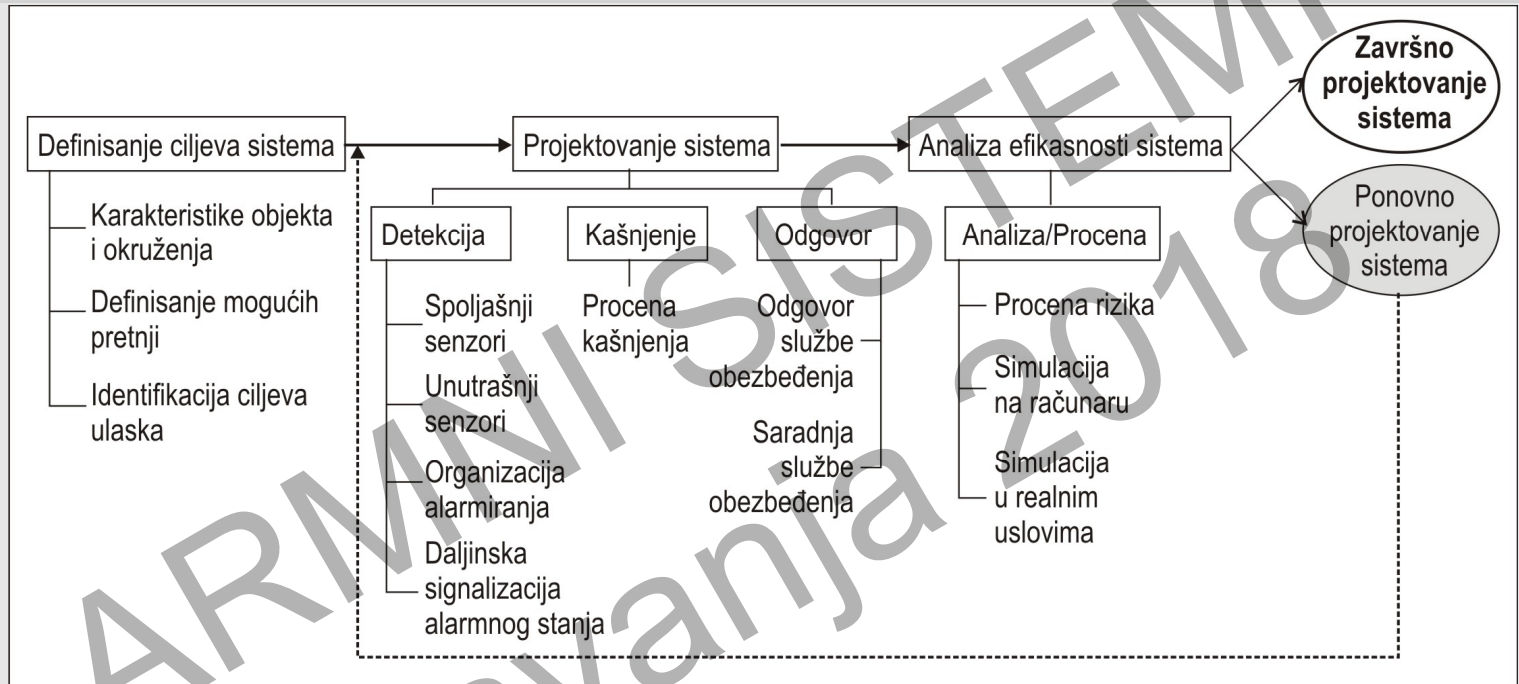
Ako je cilj da se „uljez“ onemogući pre ulaska u sam objekat, služba obezbeđenja treba da locira uljeza i bude na licu mesta za manje od 2 minuta od momenta alarmiranja. Ako je cilj da se „uljez“ uhvati „na delu“ vreme je 6 minuta, a ako je cilj da se onemogući iznošenje cilja krađe van kompleksa, vremenski okvir akcije je do 8 minuta od momenta alarmiranja.

Projektovanje sistema za zaštitu od provale



Scenario sa vremenskim dijagramom koji uključuje vreme potrebno za dolazak na mesto događaja

Projektovanje sistema za zaštitu od provale



Struktura sistema (tip detektora, broj i međusobni raspored, lokacija centrale, komunikacija, ...) zavisi najviše od:

1. *pravilno definisanih karakteristika sistema na osnovu karakteristika objekta,*
2. *karakteristika okruženja u kome se sistem instalira,*
3. *definisanja mogućih načina ulaska i*
4. *identifikaciju mogućih ciljeva provale.*

Sistemi za kontrolu pristupa – kartični sistemi

Uloga kartica:

- *Prikupljanje podataka o licu;*
- *Definisanje nivoa pristupa.*

Planiranje kontrole pristupa u objektu:

- *Potpuni pristup sa kontrolom u nekoliko pristupnih tačaka;*
- *Ograničenja u pristupu;*
- *Izuzeci od kontrole pristupa.*

Tipovi kartica:

- *Kartice sa magnetnom trakom (eng. magnetic strip);*
- *Kartice za udaljenu identifikaciju (eng. proximity cards);*
- *„Pametne“ kartice (eng. smart cards) i*
- *Kartice u dualnoj tehnologiji (eng. dual technology cards).*

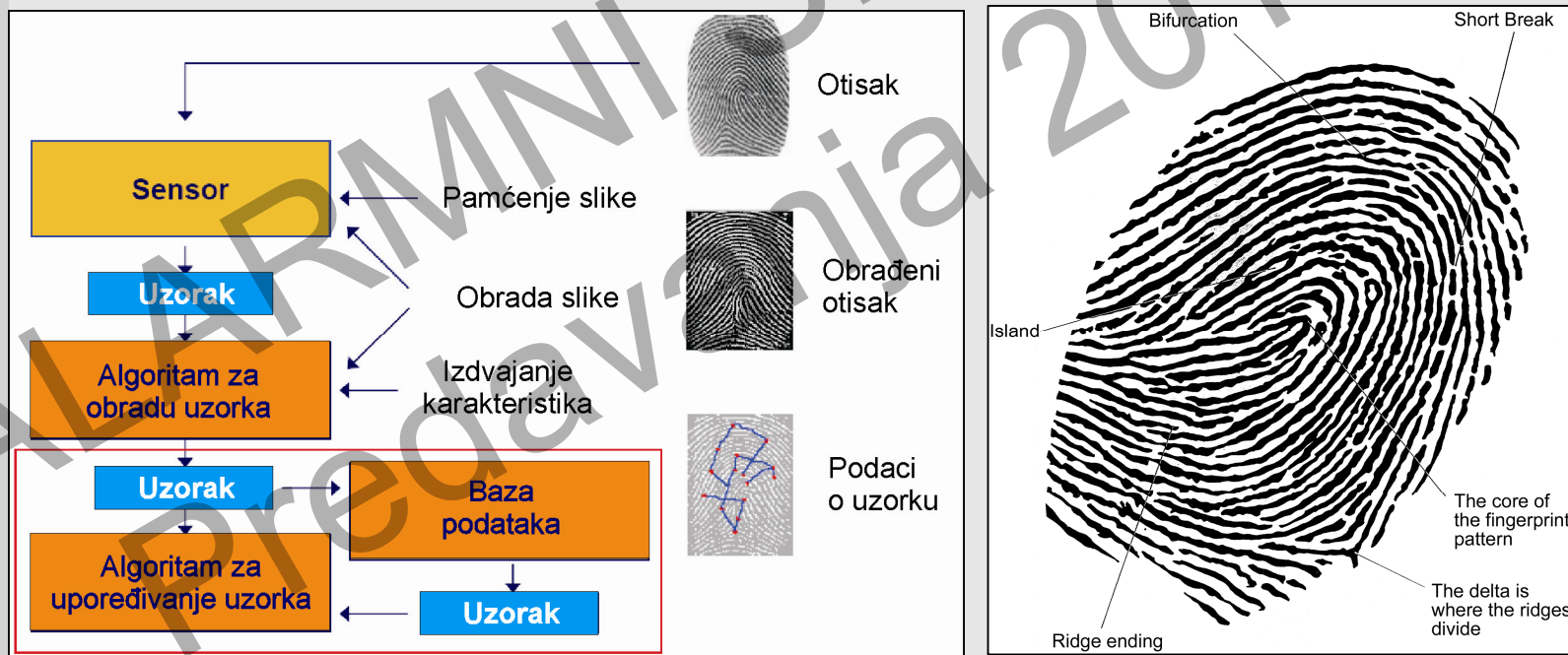


Key Name	Lock Name	Date/Time	Status	
Joe Wilson	East Entrance	03/20/2008 06:14:22 AM	Denied	
Abby Chaney	West Entrance	03/20/2008 07:28:03 AM	Key Authorized	
Pete Sussman	Records Room	03/20/2008 07:59:15 AM	Out of Schedule	
John Michaels	Computer Room	03/20/2008 08:00:03 AM	Key Authorized	
Evelyn Lefler	West Entrance	03/20/2008 08:12:16 AM	Key Authorized	
Juanita Banks	Computer Room	03/20/2008 08:18:52 AM	Key Authorized	
Andy Dunsmore	Computer Room	03/20/2008 08:27:12 AM	Denied	

- Čitači otiska prsta (eng. *fingerprint reader*);
- Čitači otiska šake (dlana), (eng. *hand geometry readers*);
- Čitači dužice oka (eng. *iris scanner*);
- Čitači mrežnjače oka (eng. *retina scanner*);
- Uređaji za prepoznavanje glasa (eng. *voice recognition*);
- Uređaji za prepoznavanje lica (eng. *facial recognition*) ;
- Ostali uređaji za biometrijsku identifikaciju (termografija lica i pojedinih delova tela, prepoznavanje hoda, ...).

Sistemi za kontrolu pristupa – biometrijska identifikacija

Čitači otiska prsta su najzastupljeniji, čine skoro 80% svih prodanih biometrijskih uređaja. Savremeni čitači otiska prsta imaju nivo greške koji je manji od 1%.



Ilustracija biometrijskog procesa identifikacije na primeru analize otiska prsta

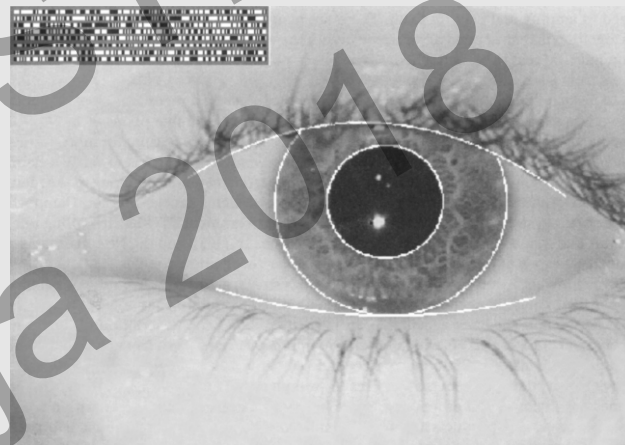
Sistemi za kontrolu pristupa – biometrijska identifikacija

Čitači otiska šake (dłana) analiziraju više od 31000 tačaka dlana i klasifikuju ih na osnovu 90 različitih kriterijuma. Merenja u čitaču uključuju širinu i dužinu šake, raspored linija na dlanu i druge karakteristike koje se upoređuju sa slikom šake koja se nalazi u bazi podataka. Procesu čitanja otiska prethodi identifikacija lica pomoću kartice.



Sistemi za kontrolu pristupa – biometrijska identifikacija

Čitači dužice oka analiziraju parametre dužice oka kao što su: vaskularna struktura i krvni sudovi, pegice, vlakna, korone, brazde i slično. Procedura takođe počinje identifikacijom pomoću kartice, posle koje je lice dužno da se približi i pogleda u sočivo kamere koje uzima uzorak.

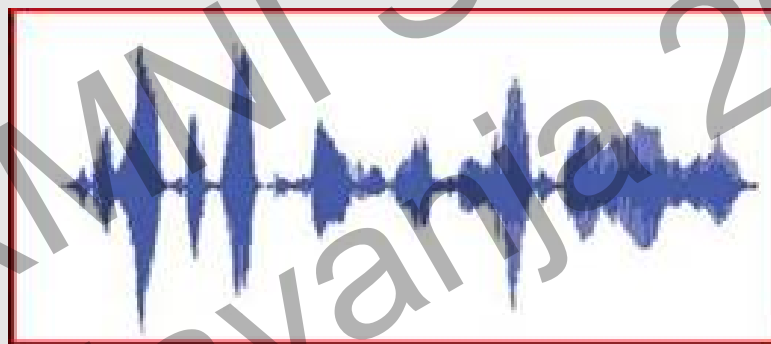


Čitači mrežnjače oka mere elemente koji predstavljaju obrazac rasporeda krvnih sudova u mrežnjači oka.



Sistemi za kontrolu pristupa – biometrijska identifikacija

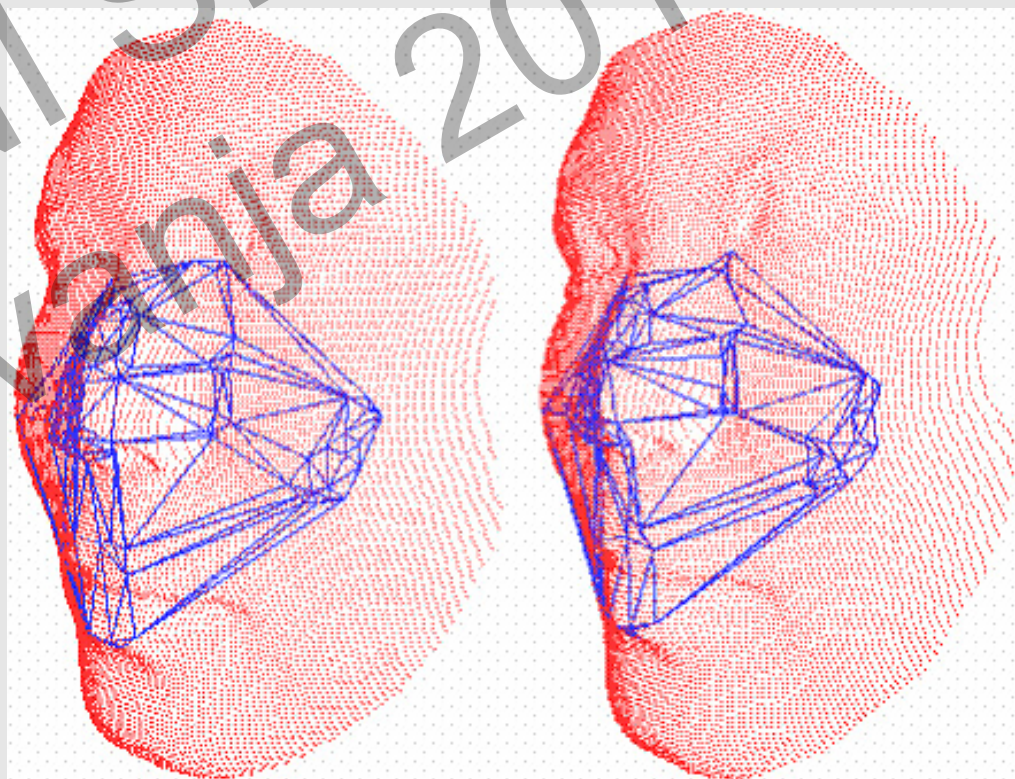
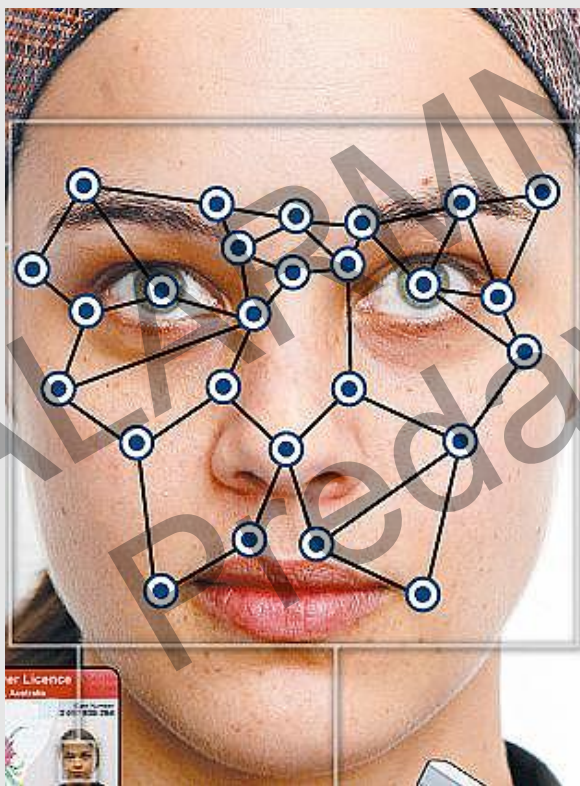
Uređaji za prepoznavanje glasa analiziraju karakteristike ljudskog govora. Govorne karakteristike nisu dovoljno jednoznačne – ne zavise samo od anatomije govornog aparata, već i od velikog broja spoljašnjih faktora, tako da ovaj metod nema visoku pouzdanost. Najčešće se koriste za identifikaciju vokalnih karakteristika u smislu otkrivanja “stranca”, tj. osobe koja nije sa određenog govornog područja.



Ilustracija digitalizovanog govornog uzorka

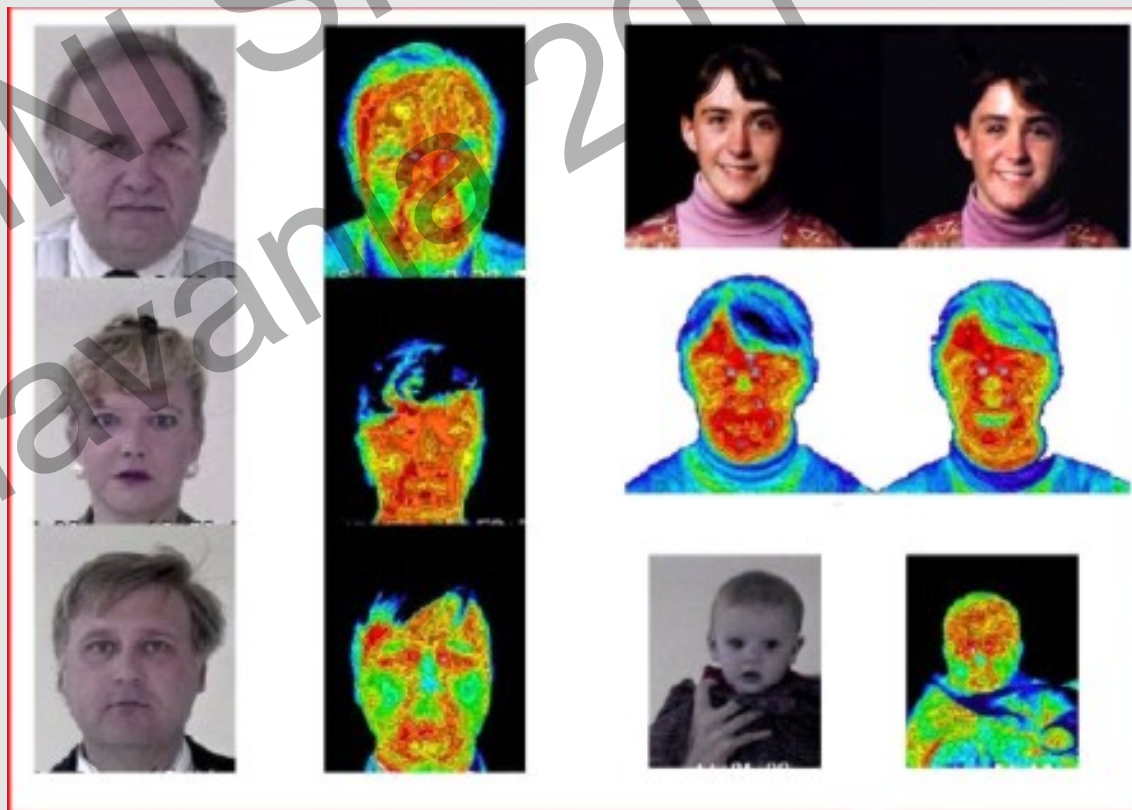
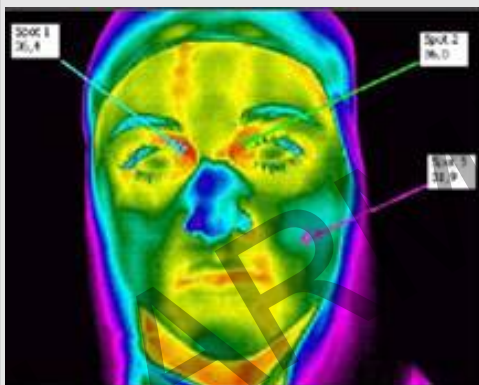
Sistemi za kontrolu pristupa – biometrijska identifikacija

Uređaji za prepoznavanje lica analiziraju karakteristične linije lica (blizu oka, nosa, usta, na čelu, itd.) i upoređuju sa zapamćenim podacima. Ovaj tip uređaja koji je do skoro smatran najmanje pouzdanim, razvojem tehnologije sve više ulazi u upotrebu.



Sistemi za kontrolu pristupa – biometrijska identifikacija

Uređaji za termografiju lica analiziraju mrežu krvnih sudova lica koja jedinstvena za svaku osobu, čak i za blizance. Prednost: visoka pouzdanost. Mane: karakteristike se mogu promeniti hirurškim zahvatom, u određenoj meri karakteristike se menjaju pod uticajem alkohola, droge i lekova, visoka cena uređaja (još uvek).



Pitanja za usmeni deo ispita

1. Osnovne mere od kojih zavisi bezbednost objekta.
2. Zaštita od provale – opšti zahtevi.
3. Mere za otkrivanje neovlašćenog ulaska i linije zaštite.
4. Nivoi zaštite u skladu sa efektima odvracanja.
5. Karakteristike sistema za zaštitu od provale.
6. Metodologija projektovanja sistema za zaštitu od provale.
7. Postupci i faze projektovanja sistema za zaštitu od provale.



Adresa za kontakt:

Dr Milan Blagojević, red. prof.

Fakultet zaštite na radu u Nišu

18106 Niš, Čarnojevića 10a

milan.blagojevic@znr fak.ni.ac.rs

Hvala na pažnji!