

# TEHNIČKI SUSTAVI SIGURNOSTI I ZAŠTITE

---

**Glavaš, Josip**

**Undergraduate thesis / Završni rad**

**2024**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **Karlovac University of Applied Sciences / Veleučilište u Karlovcu**

*Permanent link / Trajna poveznica:* <https://um.nsk.hr/um:nbn:hr:128:794862>

*Rights / Prava:* [In copyright](#)/[Zaštićeno autorskim pravom.](#)

*Download date / Datum preuzimanja:* **2024-12-27**



**VELEUČILIŠTE U KARLOVCU**  
Karlovac University of Applied Sciences

*Repository / Repozitorij:*

[Repository of Karlovac University of Applied Sciences - Institutional Repository](#)



zir.nsk.hr



DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

Veleučilište u Karlovcu  
Odjel Sigurnosti i zaštite

Stručni studij sigurnosti i zaštite

Josip Glavaš

# **TEHNIČKI SUSTAVI SIGURNOSTI I ZAŠTITE**

ZAVRŠNI RAD

Karlovac, 2024.

Karlovac University of Applied Sciences  
Safety and Protection Department

Professional undergraduate study of Safety and Protection

Josip Glavaš

# **TEHNICAL SAFETY AND PROTECTION SYSTEMS**

FINAL PAPER

Karlovac, 2024.

Veleučilište u Karlovcu  
Odjel Sigurnosti i zaštite

Stručni studij sigurnosti i zaštite

Josip Glavaš

# **TEHNIČKI SUSTAVI SIGURNOSTI I ZAŠTITE**

ZAVRŠNI RAD

Karlovac, 2024.



**VELEUČILIŠTE U KARLOVCU**  
Karlovac University of Applied Sciences

## **VELEUČILIŠTE U KARLOVCU**

Stručni studij sigurnosti i zaštite

Usmjerenje: Zaštita na radu

Karlovac, 06.2024.

### **ZADATAK ZAVRŠNOG RADA**

Student: Josip Glavaš

Matični broj: 02480818551

Naslov: Tehnički sustavi sigurnosti i zaštite

Opis zadatka:

Uvodno opisati problematiku iz naslova rada i mjesto opisa

U središnjem djelu rada kroz raspravu objasniti rizike.

Na kraju napisati zaključak.

Prilikom pisanja rada koristiti recenziranu literaturu i potpuno i pravilno citirati sve korištene izvore.

Zadatak zadan:  
Travanj, 2024.

Rok predaje rada:  
Svibanj, 2024.

Predviđeni datum obrane:  
11.07.2024.

Mentor:  
Marko Ožura, dipl.ing.

Predsjednik ispitnog povjerenstva:  
Lidija Jakšić, mag.ing.cheming.

Ovaj rad posvećujem svima koji su na bilo koji način doprinijeli mom razvoju i osposobljavanju u području sigurnosti i zaštite.

To su kolege na poslu, rukovoditelj odjela zaštite na radu kojeg sam dio te kolege i profesori na veleučilištu.

Za potrebe izrade ovog rada proučavao sam ne samo teoretske okvire već i praktične primjene u okviru svoje profesije koje mogu poboljšati kako pojedinačne tako i kolektivne sigurnosne standarde.

U okviru svog rada sudjelujem u implementaciji tehničkih sustava zaštite gdje sam stekao znanja i iskustvo na osnovu kojeg sam se iz prve ruke uvjerio da sigurnosni sustavi mogu uvelike doprinijeti podizanju razine sigurnosti i zaštite na radnom mjestu te spriječiti ozljede na radu, nezgode i nastajanje štete.

Posebnu zahvalu posvećujem svom mentoru na stručnim savjetima i podršci tijekom izrade rada.

Ovaj rad istražuje važnost integracije sustava tehničke zaštite u podizanju razine sigurnosti vezano za zaštitu na radu i općenitog podizanja svijesti o važnosti sigurnosti u kako u poslu tako i u životu.

Cilj rada je istražiti kako integracija različitih sustava tehničke zaštite može unaprijediti sigurnost u odnosu na korištenje tehničkih sustava odvojeno.

Integracija rezultira sinergijom u korist krajnjeg korisnika.

Kroz pregled literature, te informacija koje smo sakupili u praksi uz analizu relevantnih podataka identificiraju se ključne prednosti i izazovi integracije sustava tehničke zaštite.

Poseban naglasak stavljen je na identifikaciju najučinkovitijih metoda za integraciju sustava, kao i na primjere prakse iz industrije uz obvezno poštivanje zakonskih regulativa.

Potrebno je naglasiti da iako se ljudski faktor u razvoju tehničkih sustava sigurnosti umanjuje, taj faktor i dalje ostaje ključan zbog konstantne potrebe za pravilnom upotrebom sustava te zbog potrebe da se izbjegne zloupotreba sustava.

Informacije koje smo prikupili i prezentirali u ovom radu pružaju uvid u potencijalne koristi integracije sustava tehničke zaštite te također smjer u kojem se kreće politika sigurnosti na globalnoj razini.

Sigurnost i zaštita jedan je od osnovnih preduvjeta za razvoj industrije i društva općenito te je potrebno konstanto ulagati sredstva i napore u razvoj sigurnosti kako u tehničkoj tako i u drugim domenama.

## SUMMARY:

This paper explores the importance of integrating technical security systems in the context of enhancing safety and raising awareness about the importance of security both in work and in life in general.

The aim of the paper is to investigate how the integration of different technical security systems can enhance safety compared to using separate technical systems.

Integration results in synergy for the benefit of the end user.

Through a literature review and practical information gathered, along with the analysis of relevant data, key advantages and challenges of integrating technical security systems are identified.

Special emphasis is placed on identifying the most effective methods for system integration, as well as on industry practice examples with mandatory compliance with legal regulations.

It is necessary to emphasize that although the human factor in the development of technical security systems is reduced, this factor remains crucial due to the constant need for proper system usage and the need to avoid system misuse.

The information gathered and presented in this paper provide insight into the potential benefits of integrating technical security systems and also the direction of security policy at the global level.

Security and protection are fundamental prerequisites for the development of industry and society in general, and it is necessary to constantly invest resources and efforts in the development of security in both technical and other domains.



SADRŽAJ	IV
ZAVRŠNI ZADATAK .....	I
PREDGOVOR .....	II
SAŽETAK .....	III
SADRŽAJ .....	IV
1. UVOD .....	1
2. TEHNIČKA ZAŠTITA .....	2
2.1. Protuprovalno djelovanje .....	2
2.2. Protuprepadno djelovanje .....	2
2.3. Protusabotažno djelovanje .....	2
3. PROVEDBA TEHNIČKE ZAŠTITE .....	3
3.1. Tehnička sredstva i naprave .....	3
3.2. Sustav tehničke zaštite .....	4
3.3. Koraci pri provedbi tehničke zaštite .....	5
3.3.1. Snimka postojećeg stanja .....	6
3.3.2. Procjena rizika .....	6
3.3.3. Sigurnosni elaborat .....	8
3.3.4. Definiranje projektnog zadatka .....	8
3.3.5. Projektiranje sustava tehničke zaštite .....	10
3.3.6. Izvedba tehničke zaštite .....	10
3.3.7. Stručni nadzor nad izvedbom radova .....	10
3.3.8. Tehnički prijam sustava tehničke zaštite .....	11
3.3.9. Servisiranje i uporaba sustava tehničke zaštite .....	12
4. TEHNIČKI SUSTAVI ZAŠTITE .....	13
4.1. Kontrola pristupa .....	13
4.1.1. Kontroler .....	13

4.1.2.	Čitači.....	14
4.1.3.	Brava .....	14
4.1.4.	Softver za kontrolu pristupa .....	14
4.1.5.	Način rada sustava kontrole pristupa.....	15
4.2.	Evidencija radnog vremena .....	16
4.2.1.	Terminali za radno vrijeme .....	17
4.2.2.	Napajajući i komunikacijski pretvornici .....	18
4.2.3.	Softver .....	18
4.2.4.	Način rada sustava evidencije radnog vremena .....	19
4.3.	Sustavi digitalne portafonije .....	20
4.3.1.	Prednosti sustava digitalne portafonije .....	20
4.3.2.	Komponente sustava portafonije .....	20
4.3.3.	Način rada sustava digitalne portafonije .....	22
4.4.	Sustavi čitanja registarskih oznaka za garaže.....	23
4.5.	Videonadzor .....	25
4.5.1.	Primjena sustava videonadzora.....	26
4.5.2.	Komponente sustava videonadzora.....	26
4.5.3.	Grafički prikaz sustava videonadzora .....	27
4.5.4.	Tipovi kamera .....	28
4.5.5.	Tipovi snimača .....	30
4.5.6.	Softver .....	30
4.6.	Protuprovalni sustav.....	31
4.6.1.	Signalizacija.....	31
4.6.2.	Način rada protuprovalnog sustava .....	31
4.7.	Sustavi vatrodjave .....	32
4.7.1.	Komponente vatrodjavnog sustava.....	33

4.8.	Sustavi evakuacije.....	34
4.9.	Sustavi hidrantskih mreža za gašenje požara .....	36
4.9.1.	Unutarnja hidrantska mreža .....	36
4.9.2.	Vanjska hidrantska mreža.....	38
4.10.	Stabilni sustavi gašenja .....	39
5.	INTEGRACIJA .....	41
5.1.	Kontrola pristupa i evidencije radnog vremena .....	44
5.2.	Centralni dojavni sustav .....	44
5.3.	Sustav digitalne portafonije .....	45
5.4.	Videonadzor i vatrodojava.....	45
5.5.	Vatrodojava i protuprovala .....	45
5.6.	Sprinkleri, vatrodojava i gašenje požara.....	46
6.	PRAVILNICI I ZAKONI.....	49
7.	ZAKLJUČAK .....	50
8.	LITERATURA .....	51
9.	PRILOZI.....	53
9.1.	Popis slika .....	53
9.2.	Popis tablica .....	54

## 1. UVOD

U današnjem sve složenijem i povezanijem svijetu, sigurnost i zaštita postali su ključni elementi za očuvanje društvene stabilnosti i osobne sigurnosti. Tehnički sustavi sigurnosti i zaštite igraju vitalnu ulogu u osiguravanju sigurnosti ljudi, imovine i podataka.

Kroz povijest, razvoj sigurnosnih tehnologija od jednostavnih mehaničkih sustava do sofisticiranih digitalnih rješenja omogućila je sveobuhvatniji pristup zaštiti i sigurnosti.

Sigurnosni sustavi imaju presudnu ulogu u sprečavanju neovlaštenih ulazaka i zaštiti imovine. Praćenje radnog vremena omogućuje nadzor prisutnosti i učinkovitosti zaposlenika. Sustavi kontrole pristupa osiguravaju da samo ovlaštene osobe mogu ulaziti u određene prostore, dok sustavi za dojavu požara omogućuju rano otkrivanje vatre i automatsko otključavanje vrata za hitnu evakuaciju. Video nadzor služi za kontinuirano praćenje i dokumentiranje događaja, čime se poboljšava sigurnost i omogućuje brza reakcija na incidente.

Kombiniranjem novih tehnologija olakšava se identifikacija i reakcija na sigurnosne prijetnje i poboljšava koordinacija rada službi održavanja i sigurnosti u kombinaciji sa tehničkim sustavima sigurnosti.

Da bi se postigla maksimalna razina optimalnog rada sigurnosnih sustava potrebna je pravilna integracija i povezivanje sustava, kad se ispune ti zahtjevi postiže se značajno povećanje razine sigurnosti.

## **2. TEHNIČKA ZAŠTITA**

Tehnička zaštita podrazumijevaju skup više radnji koje na posredan ili neposredan način djeluju radi zaštite ljudi, njihove imovine ili oboje. Osnovni cilj tehničke zaštite je da se spriječe protupravne i druge radnje koje mogu naštetiti osobama ili njihovoj imovini, a to su protuprovalno, protuprepadno i protusabotažno djelovanje [1].

### **2.1. Protuprovalno djelovanje**

Najvažnija uloga za protuprovalno djelovanje pripada raznim detektorima kojima je zadatak otkriti neželjeni ulazak u objekt i o tome obavijestiti korisnika. Detektori se svrstavaju u one za unutrašnju i one za vanjsku zaštitu prolaza i otvora a dijelimo ih na detektore kretanja, detektore vibracija i detektore otvaranja.

### **2.2. Protuprepadno djelovanje**

Svrha protuprepadnog djelovanja je zaštititi objekt s ciljem odvracanja provalnika prije nego je došlo do provale u štice objekta. Na ovakve detektore se postavljaju visoki zahtjevi, a to su velika pouzdanost te velika autonomija i mala osjetljivost prema vanjskim utjecajima, s obzirom da štite prostore velikih površina.

### **2.3. Protusabotažno djelovanje**

Protusabotažnim djelovanjem se štiti oprema i sustavi tehničke zaštite koje koristimo, softwareski ili hardwareseki sustavi.

### 3. PROVEDBA TEHNIČKE ZAŠTITE

Provedba tehničke zaštite realizira se tehničkim napravama i sredstvima, te njihovim povezivanjem u cjelinu, tj. cjelokupnim sustavom tehničke zaštite, a provodi se kroz više koraka [1].

#### 3.1. Tehnička sredstva i naprave

- 1) Uređaji za fizičko i mehaničko sprječavanje nedopuštenog ulaska u štíćene objekte i prostore
  - rampe, specijalne barikade, građevne konstrukcije, ograde
  - protuprovalna vrata
  - brave sa serijskim brojevima ili kodovima
  - stakla koja su neprobojna
  - trezori i slični uređaji za čuvanje vrijednosti
  - elektroničke i mehaničke naprave kao što su uređaji za detekciju metalnih predmeta



*Slika 3.1. Prikaz protuprovalnih vrata [3]*

2) elektronički sustavi:

- protuprovalni sustavi
- dojavljivači koji se instaliraju na sustave sigurnosti
- kontrolni sustavi
- sustavi video nadzora
- sustavi centralnog prijama
- signalizacije alarma



*Slika 3.2. Prikaz kontrolne sobe, centralni dojavni sustav [4]*

- 3) tehnička sredstva za zaštitu ljudi kao što su protuprepadni alarmi
- 4) protusabotažni elementi kao što su specijalna ogledala za pregled vozila

### **3.2. Sustav tehničke zaštite**

Kako bi se na što efikasniji i sigurniji način zaštitilo od neželjenih radnji, poželjno je koristiti više sredstava i uređaja povezanih u funkcionalnu cjelinu, a takva funkcionalna cjelina čini sustav tehničke zaštite. Zaštita povjerljivih informacija i podataka se u ovom slučaju ističe jer je potreba još veća razina

zaštite tj. moraju biti ispunjene najmanje tri razine zaštite. Fizička zaštita (radi se o zabrani pristupa prostorima u kojima su povjerljivi podaci i informacije).

Hardverska zaštita u koju spada mehanička zaštita računala) i softverska zaštita, što je u najčešćem slučaju zaštita pomoću lozinki.



*Slika 3.3. Simbolika softverske zaštite [5]*

### **3.3. Koraci pri provedbi tehničke zaštite**

Tehnička zaštita provodi se isključivo unutar kruga zaštite tzv. perimetra.

Elementi koji su bitni pri provedbi tehničke zaštite su sljedeći:

- snimka postojećeg stanja štice objekta
- izrada procjene rizika
- izrada sigurnosnog elaborata
- definiranje projektnog zadatka
- projektiranje sustava tehničke zaštite
- izvedbu sustava tehničke zaštite
- stručni nadzor nad izvedbom radova
- obavljanje tehničkog prijama sustava tehničke zaštite
- servisiranje sustava tehničke zaštite
- uporaba sustava tehničke zaštite
-



### 3.3.1. Snimka postojećeg stanja

Snimka postojećeg stanja šticeenog objekta i analiza problema temelje se na prikupljenim podacima o postojećim mjerama zaštite, broju, vrsti i načinu izvršenja dosadašnjih štetnih događaja te visini šteta prouzročenih tim događajima.

### 3.3.2. Procjena rizika

3.3.2. Procjena rizika izrađuje se primjenom priznatih pravila u provedbi tehničke zaštite. Priznata pravila uključuju odgovarajuće hrvatske norme, a u slučaju njihovog nedostatka primjenjuju se odgovarajuće europske ili međunarodne norme.

Procjena rizika izrađuje se na temelju podataka [1]:

- vrsti, namjeni, veličini i izgledu objekta, lokaciji i okruženju te građevnim i ostalim svojstvima objekta,
- vrsti i broju stalnih i povremenih korisnika,
- režimu rada i načinu korištenja objekta i
- opremi, predmetima i dokumentima koji će se u objektu nalaziti ili se već nalaze te stupnju rizika od njihova oštećenja, otuđenja ili uništenja.

Prema podacima za izradu procjene rizika šticeeni objekti se kategoriziraju u 6 kategorija, koje sadrže obvezne mjere zaštite.

Prva kategorija zaštite je najviši stupanj zaštite, a kao zaštitu predviđa [1]:

- tehničku i mehaničku zaštitu kojom se signalizira neovlašten ulazak u šticeeni prostor, te se dojavljuje na Centralni dojavni sustav,
- tehničku zaštitu kojom se prati kretanje u šticeenom prostoru i pojedinačno šticeenim prostorijama (kontrola prolaza i video nadzor) uz videozapis,
- zaštitu pojedinačnih vrijednosti pomoću specijalnih kasa, trezora i sl.,

- integralnu zaštitu s najmanje jednim lokalnim nadzornim mjestom i sustavom veze sa zaštitarima na štíćenom objektu i
- sigurnosni Plan postupanja i procedure u slučajevima pretpostavljenih incidentnih situacija.

Druga kategorija predstavlja visoki stupanj zaštite, a kao zaštitu predviđa [1]:

- tehničku i mehaničku zaštitu kojom se signalizira neovlašten ulazak u štíćeni prostor, te se događuje na Centralni dojavni sustav,
- zaštitu kojom se prati kretanje u štíćenom prostoru (kontrola prolaza i video nadzor) uz videozapis i
- integralnu zaštitu s najmanje jednim lokalnim nadzornim mjestom i sustavom veze sa Centralnim dojavnim sustavom.

Treća kategorija predstavlja viši stupanj zaštite, a kao zaštitu predviđa [1]:

- tehničku i mehaničku zaštitu kojom se signalizira neovlašten ulazak u štíćeni prostor, te se događuje na Centralni dojavni sustav i
- tehničku zaštitu kojom se prati kretanje u štíćenom prostoru (kontrola prolaza i videonadzor) uz videozapis.

Četvrta kategorija predstavlja srednji stupanj zaštite, a kao zaštitu predviđa [1]:

- mehaničku i tehničku zaštitu kojom se na licu mjesta zvučno ili svjetlosno signalizira neovlašten ulazak u štíćeni prostor i
- video nadzor kojim se prati kretanje u štíćenom prostoru uz video zapis.

Peta kategorija predstavlja niži stupanj zaštite, i on predviđa [1]:

- mehaničku i tehničku zaštitu kojom se na licu mjesta zvučno ili svjetlosno signalizira neovlašten ulazak u štíćeni prostor.

Šesta kategorija predstavlja minimum zaštite, a obuhvaća [1]:

- mehaničku zaštitu bez uporabe elektroničkih naprava,
- cilindarske brave i
- obične ograde bez tehničkih elemenata.

### **3.3.3. Sigurnosni elaborat**

Na temelju izrađene procjene rizika izrađuje se sigurnosni elaborat. Sigurnosnim elaboratom određuje se razina tehničke zaštite, integralne zaštite te povezanost s ostalim tehnološkim sustavima na objektu. Sigurnosnim elaboratom utvrđuju se mjere i postupci potrebni za učinkovitu zaštitu objekta koji spadaju u dvije skupine.

- 1) zahtjevi koje moraju ispunjavati sustavi koji nisu sustavi tehničke zaštite, ali utječu na sigurnost objekta i pouzdan rad sustava tehničke zaštite
- 2) građevni i slični zahtjevi od značaja za pravilan i pouzdan rad sustava tehničke zaštite

### **3.3.4. Definiranje projektnog zadatka**

Na temelju izrađenog i posebnih zahtjeva korisnika objekta izrađuje se projektni zadatak. Projektnim zadatkom utvrđuju se potrebni parametri za izradu projekta sustava tehničke zaštite, a osobito tehničke specifikacije, opseg rada, potrebna oprema, rokovi za izvedbu i kriteriji za procjenu učinkovitosti koji se mogu podijeliti u četiri različite discipline:

- vrsta tehničke zaštite
- smještaj centra tehničke zaštite
- smještaj uređaja i opreme
- način polaganja instalacija

Projektni zadatak	
Broj projekta:	Naziv projekta: Proces proizvodnje u radionici čeličnih konstrukcija
Nalog za projekt izdao:	Voditelj projekta:
EMKON Metalne konstrukcije d.o.o.	Josip Popović
Članovi projektnog tima:	
Josip Popović, Mateo Mikulić	
<p><b>Ciljevi projekta:</b>            Stjecanje praktičnih znanja o procesima izrade čeličnih konstrukcija, koje uključuje:            -tehničke pripreme proizvodnje            -processe dopremanja i skladištenja materijala            -processe obrade čeličnih profila, pripreme čeličnih sklopova i podsklopova.            Stjecanje iskustva i radno osposobljavanje kroz pripremu radioničkih crteža u programima AutoCad i SolidWorks.</p> <p><b>Faze projekta</b></p> <ul style="list-style-type: none"> <li>- Upoznavanje sa procesima izrade čeličnih konstrukcija</li> <li>- Upoznavanje tehničke pripreme proizvodnje</li> <li>- Upoznavanje sa procesima dopreme, skladištenja i obrade čeličnih profila</li> <li>- Rad u programima AutoCad i SolidWorks</li> <li>- Programiranje plinske i plazma CNC rezačice</li> <li>- Samostalno odrađena jednostavna čelična konstrukcija</li> </ul>	
<p><b>Koristi od projekta:</b></p> <ul style="list-style-type: none"> <li>- Upoznavanje sa procesom proizvodnje izrade čeličnih konstrukcija</li> <li>- Praktični rad na projektom zadatku koristeći vještine programa AutoCad i SolidWorks</li> <li>- Praktični rad na CNC plinskoj i plazma rezačici</li> <li>- Stjecanje praktičnih znanja i iskustava za buduće zapošljenje</li> </ul>	
<p><b>Termini početka projekta:</b> Prema dogovoru  <b>Termin završetka projekta:</b> Prema dogovoru  <b>Ukupno efektivnih sati na projektu:</b> 120-240 sati</p>	
Ukupno trajanje projekta u danima: 15-30 dana	Budžet projekta:
EMKON Metalne konstrukcije d.o.o.	Josip Popović dipl. ing. strojarstva
Nalogodavac projekta	Voditelj projekta
<p><b>Prilozi:</b></p> <input type="checkbox"/> Mrežni plan projekta <input type="checkbox"/> Ograničenja <input type="checkbox"/> Produkti projekta <input type="checkbox"/> Prijetnje	

*Slika 3.4. Primjer izgleda projektnog zadatka [6]*

### **3.3.5. Projektiranje sustava tehničke zaštite**

Projektiranje sustava uključuje odabir vrste i opsega zaštite koju ćemo implementirati, odabir opreme, razradu koncepcije tehničke zaštite te izradu potrebne dokumentacije. Projektnu dokumentaciju smiju izrađivati samo pravne i fizičke osobe registrirane za obavljanje poslova tehničke zaštite. Projekt sustava tehničke zaštite mora biti izrađen sukladno propisima koji uređuju poslove projektiranja. Analiza trenutnog stanja štíćenog objekta, zajedno s procjenom rizika i sigurnosnim elaboratom, te definiranje projektnih zadataka, čine sastavni dio projekta sustava tehničke zaštite.

### **3.3.6. Izvedba tehničke zaštite**

Izvođenje sustava tehničke zaštite uključuje postavljanje instalacija, montažu opreme, programiranje, podešavanje, ispitivanje i probno pokretanje sustava, kao i verifikaciju opreme i sustava te tehnički prijem. Osim toga, obuhvaća i izradu uputa za rukovanje i obuku osoblja.

Tehnička zaštita obavlja svoju djelatnost isključivo na temelju radnih naloga.

Radni nalog mora sadržavati slijedeće podatke [1]:

- ime i prezime zaštitara,
- tvrtku trgovačkog društva ili obrta,
- opis posla i broj ugovora,
- vrijeme početka i završetka posla i
- potpis odgovorne osobe.

### **3.3.7. Stručni nadzor nad izvedbom radova**

Zaštitar je obvezan imati kod sebe nalog propisanog sadržaja i zaštitarsku iskaznicu za vrijeme dok obavlja dužnost. U izradi tehničke zaštite, stručno osoblje, poput nadzornog inženjera, odgovorno je za osiguranje da se svi radovi provode u skladu s projektnom dokumentacijom i relevantnim zakonima.

### 3.3.8. Tehnički prijam sustava tehničke zaštite

<hr/> <p>(NAZIV I SJEDIŠTE TRGOVAČKOG DRUŠTVA ILI OBRTRNIKA)</p>	
<p>Na temelju članka 22. stavka 3. Pravilnika o uvjetima i načinu provedbe tehničke zaštite ("Narodne novine", br. __/__.) sastavlja se</p>	
<p><b>Z A P I S N I K</b></p>	
<p>o obavljenom tehničkom prijemu naprava i sustava tehničke zaštite prema Ugovoru broj:</p>	
<hr/> <p>(broj Ugovora)</p>	
<p>sklopljenog sa:</p>	
<hr/> <p>(naziv i sjedište pravne osobe ili adresa obrtnika)</p>	
<p>Prilikom prijama naprave/uređaja/sustava tehničke zaštite je utvrđeno:</p>	
<ol style="list-style-type: none"><li>1. da je ugrađena naprava/uređaj/elementi sustava tehničke zaštite u ispravnom stanju i u funkciji za koju su namijenjeni;</li><li>2. da je ugradnja naprave ili uređaja izvedena sukladno skici (crtežu);</li><li>3. da je sustav tehničke zaštite usklađen sa projektom;</li><li>4. da je osoba/osoblje koje upravlja napravom/uređajem/sustavom tehničke zaštite obučeno za taj posao;</li><li>5. da su korisničke upute uručene vlasniku ili korisniku objekta i da su iste komplementarne s ugrađenim elementima;</li><li>6. da su certifikati i potvrde koje dokazuju kvalitetu ugrađene opreme provjereni i uručeni vlasniku ili korisniku objekta.</li></ol>	
<p>U _____ (mjesto i datum)</p>	
Za naručitelja:	Za izvođača:
_____	_____
(potpis naručitelja)	(potpis ovlaštenog predstavnika izvođača)

Slika 3.5. Zapisnik o obavljenom tehničkom prijemu [1]

Tehnički prijam sustava tehničke zaštite podrazumijeva [1]:

- provjeru ispravnosti i funkcionalnosti svih uređaja i opreme koji čine sustav tehničke zaštite,
- provjeru usklađenosti sustava tehničke zaštite sa projektom, odnosno skicom,
- provjeru obučenosti osoblja,
- provjeru korisničkih uputstava za rukovanje i
- provjeru dokaza kvalitete ugrađene opreme.

Tehnički prijam obavlja ovlaštenu predstavnik vlasnika ili korisnika objekta i izvođača. O obavljenom tehničkom prijemu sastavlja se zapisnik. Primjer zapisnika prikazan je slikom 3.5.

### **3.3.9. Servisiranje i uporaba sustava tehničke zaštite**

Vlasnik ili korisnik objekta koji je pod zaštitom dužan je održavati u ispravnom stanju instalirani sustav tehničke zaštite i sve njegove dijelove. Osim toga, treba osigurati godišnje servisiranje sustava. Poslove održavanja i servisiranja sustava tehničke zaštite mogu obavljati samo pravne i fizičke osobe registrirane za te poslove. Odgovornost izvođača je osigurati održavanje i servisiranje sustava tijekom jamstvenog roka, te po potrebi ponuditi održavanje i servisiranje i izvan tog roka, prema zahtjevu korisnika. Vlasnik ili korisnik objekta koji je opremljen video nadzorom dužan je osigurati da se na vidnom mjestu pri ulasku u objekt, kao i unutar prostorija, istakne obavijest posjetiteljima o prisutnosti sustava tehničke zaštite. Nadalje, vlasnik ili korisnik objekta ne smije koristiti osobne podatke prikupljene sustavom video nadzora izvan zakonski propisane namjene.

## 4. TEHNIČKI SUSTAVI ZAŠTITE

Za efikasnu i sigurnu zaštitu od neželjenih događaja preporučljivo je koristiti različita sredstva i uređaje koji su povezani u funkcionalnu cjelinu, što čini sustav tehničke zaštite. Integracijom više sustava zaštite u jednu cjelinu omogućuje se sveobuhvatna zaštita objekta. Neki od tehničkih sustava zaštite su: kontrola pristupa, videonadzor, sustavi protuprovale, sustavi vatrodjave, sustavi kontrole radnog vremena, sustavi čitanja registarskih oznaka za garaže, sustavi hidrantskih mreža za zaštitu od požara, stabilni sustavi gašenja, evakuacija i drugi sustavi. U nastavku ću opisati svaki od sustava.

### 4.1. Kontrola pristupa

Kontrola pristupa predstavlja osnovu vezano za rad sustava sigurnosti. Kada je potrebno ograničiti pristup zaposlenicima ili posjetiteljima, ili osigurati da samo određeni zaposlenici imaju pravo pristupa određenim prostorijama, nužno je implementirati sustav kontrole pristupa. Sustav kontrole pristupa može se podijeliti na četiri osnovne komponente. To su kontroleri, čitači, brave i softver.

#### 4.1.1. Kontroler

Kontroler je osnova sustava koje povezuje čitače, brave i komunicira sa softverom za kontrolu pristupa.



*Slika 4.1. Kontroler sustava kontrole pristupa [7]*



#### 4.1.2. Čitači

Za identifikaciju korisnika koriste se čitači. Često se koriste RFID čitači za identifikaciju putem kartica, koda ili biometrijski čitači za identifikaciju putem otiska prsta.



*Slika 4.2. RFID čitač s tipkovnicom [7]*

#### 4.1.3. Brava

Električne ili elektromagnetne brave su najčešće korištene u sustavima tehničke zaštite. Povezuju se na kontroler kao i čitači te omogućuju otvaranje vrata nakon uspješne identifikacije korisnika.



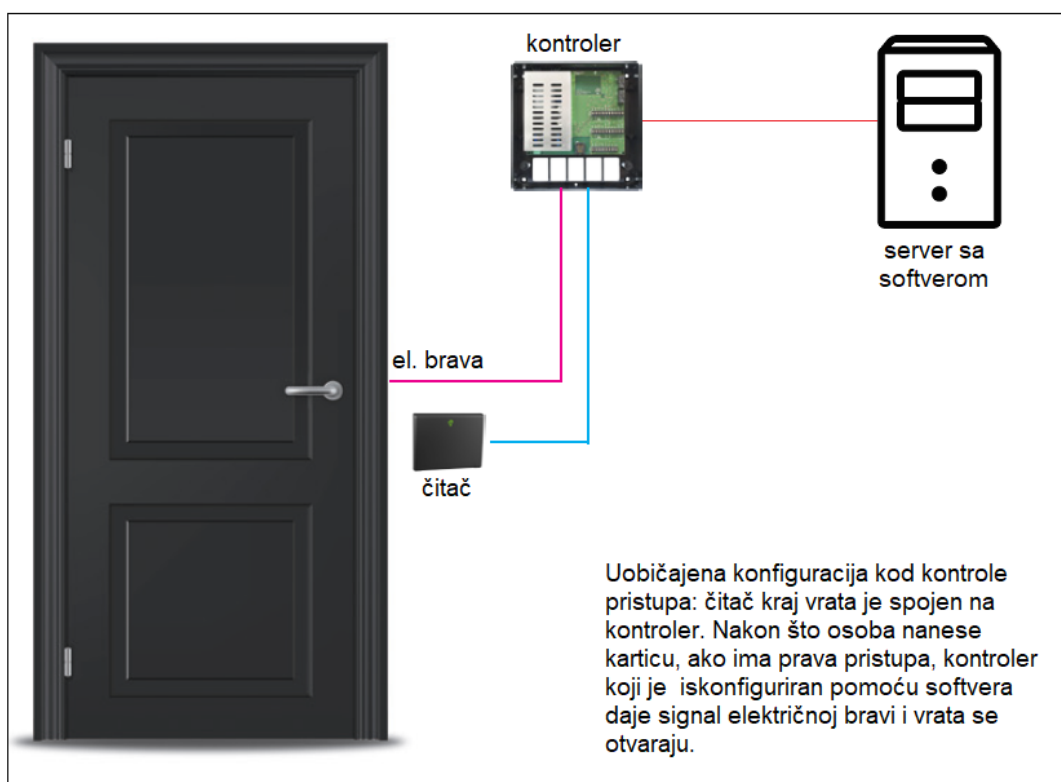
*Slika 4.3. Primjer elektromagnetske (lijevo) i električne (desno) brave [7]*

#### 4.1.4. Softver za kontrolu pristupa

Softver koristimo za upravljanje sustavom kontrole pristupa, što uključuje dodavanje ili brisanje korisnika, određivanje njihovih prava pristupa, generiranje izvještaja o prolascima i druge administrativne funkcije.

#### 4.1.5. Način rada sustava kontrole pristupa

Na ulazima u prostorije za koju želimo ograničiti pristup se instaliraju čitači preko kojih će se vršiti identifikacija osoba. Električne ili elektromagnetne brave na vratima su povezane s kontrolerima isto kao i čitači. Kada osoba prinese svoju ID karticu ili otisak prsta, kontroler provjerava autorizaciju te osobe u bazi podataka. Ako osoba ima autorizaciju, kontroler daje signal električnoj bravi i vrata se otvaraju. Ako osoba nema odgovarajuću autorizaciju, vrata ostaju zatvorena.



Slika 4.4. Grafički prikaz procesa kontrole pristupa [7]

Svaki djelatnik ili posjetitelj može imati dopušten pristup samo određenim prostorijama, na primjer, skladištaru se može omogućiti otvaranje vrata skladišta, ali ne i ulazak u server salu. Također se može ograničiti pristup prostorijama samo na određene vremenske intervale, na primjer, pristup skladištu je moguć samo radnim danom od 8 do 16 sati.

Sustave kontrole pristupa možemo podijeliti na:

- sustave s beskontaktnim karticama
- biometrijske sustave

U slučaju sustava kontrole pristupa sa beskontaktnim karticama omogućeno je precizno i brzo ograničavanje pristupa za pojedine prostore. Putem softvera iz web preglednika moguće je u realnom vremenu pratiti koje su kartice korištene za pristup određenim prostorijama. Također, dodavanje i brisanje prava pristupa za određene prostore obavlja se putem web sučelja. Sustavi kontrole pristupa prema otisku prsta vrše identifikaciju pojedinih djelatnika/posjetitelja po principu biometrije. Usporedbom biometrijskih karakteristika spremljenih otisaka prstiju sa trenutnim otiskom vrši se identifikacija korisnika, te se na temelju njegovih prava dopušta ili odbija ulazak u određeni prostor. Za identifikaciju putem otiska prsta potrebni su čitači s ugrađenim skenerima otisaka prstiju.



*Slika 4.5. Čitač otiska prstiju pri sustavu kontrole pristupa [7]*

## **4.2. Evidencija radnog vremena**

Evidencija radnog vremena važan je element kako za zaposlenike tako i za poslodavce. Sustav evidencije radnog vremena svojim učinkom direktno i indirektno doprinosi racionalizaciji i organizaciji rada, te pospješuje ukupnu produktivnost i učinkovitost. Sustav evidencije funkcionira tako da se prate vremena prijave i odjave te na osnovu unaprijed određenih pravila radi obračun sati. Prema specifičnim zahtjevima klijenta, prilagođavamo različite rasporede radnog vremena za različite vrste zaposlenika. Na primjer, za recepciju koja je

otvorena 24 sata i ima radnike u smjenama, koristimo smjenski radni model. Za zaposlenike u uredima s radnim vremenom od 8 do 16 sati, primjenjujemo fiksni radni raspored. Unutar ovih rasporeda moguće je definirati i dodatne elemente, poput vremena za pauzu ili izlazak iz ureda iz poslovnih ili privatnih razloga.

Neke od prednosti evidencije radnog vremena [8]:

- trenutan obračun prekovremenih sati,
- smanjenje troškova vođenjem ručne evidencije,
- smanjenje kašnjenja djelatnika,
- optimizacija i olakšano planiranje poslovnih procesa,
- kontrola odsutnosti djelatnika i
- smanjenje administracije.

Sustavi za kontrolu radnog vremena sastoje se od nekoliko komponenti. To su terminali za radno vrijeme, uređaji za napajanje, komunikacijski pretvornici i softver za evidenciju radnog vremena.

#### 4.2.1. Terminali za radno vrijeme

Obično se koriste za identificiranje putem kartica ili putem otiska prsta.



Slika 4.6. Primjer RFID terminala i terminala s čitačem otiska prsta [8]

#### 4.2.2. Napajачi i komunikacijski pretvornici

Napajanje uređaja za evidentiranje radnog vremena obično se odvija putem serijske RS-485 komunikacije. Ti uređaji također služe za pretvaranje serijske komunikacije u TCP/IP, omogućujući terminalima komunikaciju s odgovarajućim softverom.



*Slika 4.7. Napajanje za jedan terminale [8]*

#### 4.2.3. Softver

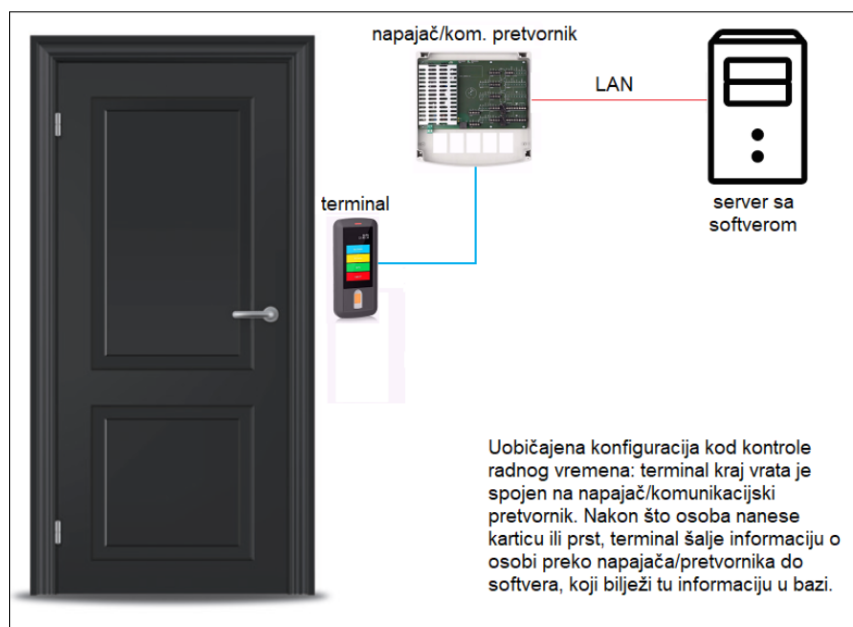
Softver se koristi za upravljanje sustavom evidencije radnog vremena, što uključuje definiranje vremenskih intervala, dodavanje i micanje radnika iz evidencije, generiranje izvještaja o radnom vremenu i slično. Sustavi se također mogu podesiti da sami generiraju određene podatke koji su nam potrebni ni također ih je moguće spojiti s nekim drugim sustavom kao što je kontrola pristupa da bi se onemogućio ulazak u određeni prostor bez da je obavio evidentiranje.



Slika 4.8. Jantar Codeks TA aplikacija za radno vrijeme [8]

#### 4.2.4. Način rada sustava evidencije radnog vremena

Na ulazu u tvrtku postavlja se terminal za evidenciju radnog vremena, putem kojeg zaposlenici registriraju dolazak i odlazak s posla. Terminal je spojen na napajanje i komunikacijski pretvornik, koji je integriran u lokalnu mrežu (LAN) i prenosi informacije do računala s instaliranim softverom za evidenciju radnog vremena. Kada zaposlenik prinese svoju ID karticu ili otisak prsta, terminal šalje informaciju o zaposleniku preko pretvornika do softvera, koji zatim bilježi tu informaciju u bazi podataka.



Slika 4.9. Grafički prikaz procesa sustava evidencije radnog vremena [8]

### **4.3. Sustavi digitalne portafonije**

Stari analogni sustavi portafonije omogućavali su samo dvosmjernu glasovnu komunikaciju. Sustavi digitalne portafonije omogućuju da, uz glasovnu komunikaciju, i vidimo posjetitelja pomoću videa koji se šalje sa vanjske jedinice na unutarnju. Na ovaj način se ostvaruje i vizualna identifikacija posjetitelja prije nego što mu se dozvoli ulaz u prostor [9].

#### **4.3.1. Prednosti sustava digitalne portafonije**

Digitalna portafonija nudi niz prednosti u odnosu na klasične analogne sustave:

- video visoke rezolucije s mogućnošću pohrane snimke,
- mogućnost korištenja postojeće digitalne mrežne infrastrukture,
- mogućnost zvanja više unutarnjih jedinica sa jednom vanjskom jedinicom (npr. jedna tipka zove četiri unutarnje jedinice),
- mogućnost zvanja jedne unutarnje jedinice sa više vanjskih jedinica,
- mogućnost primanja poziva i slike uživo na mobitel te udaljenog otključavanja vrata,
- pregled kompatibilnih digitalnih kamera sa unutarnje jedinice,
- mogućnost spajanja alarmnih uređaja na unutarnju jedinicu (npr. detektora ugljičnog monoksida ili vatrodojavnog detektora) i
- prikaz slike uživo bez ostvarivanja poziva.

#### **4.3.2. Komponente sustava portafonije**

Komponente sustava portafonije su:

- elektroprihvatnik
- napajanje unutarnja
- vanjska jedinica

Elektroprihvatnik se ugrađuje u dovratnik. Kod modernijih rješenja vrata se mogu otvarati i pomoću mobitela ili pomoću čitača kartica (ako ga vanjska jedinica podržava). Kod napajanja, neke vanjske i unutarnje jedinice se napajaju putem PoE-a, pa nije potrebno dodatno napajanje. Ako je potrebno, obično se radi o 12 voltnom napajanju.

Vanjska jedinica se postavlja ispred ulaza u zgradu, moguće je podžbukno ili nadžbukno montiranje. Može imati jednu ili više pozivnih tipki, a za veće objekte može sadržavati i bročanu tipkovnicu. Obično je vanjska jedinica povezana s elektroprihvatom koji se privremeno otpušta kada domaćin odobri ulazak posjetitelju.



*Slika 4.10. Primjer vanjske jedinice s jednom tipkom (lijevo) i s tipkovnicom (desno) [9]*

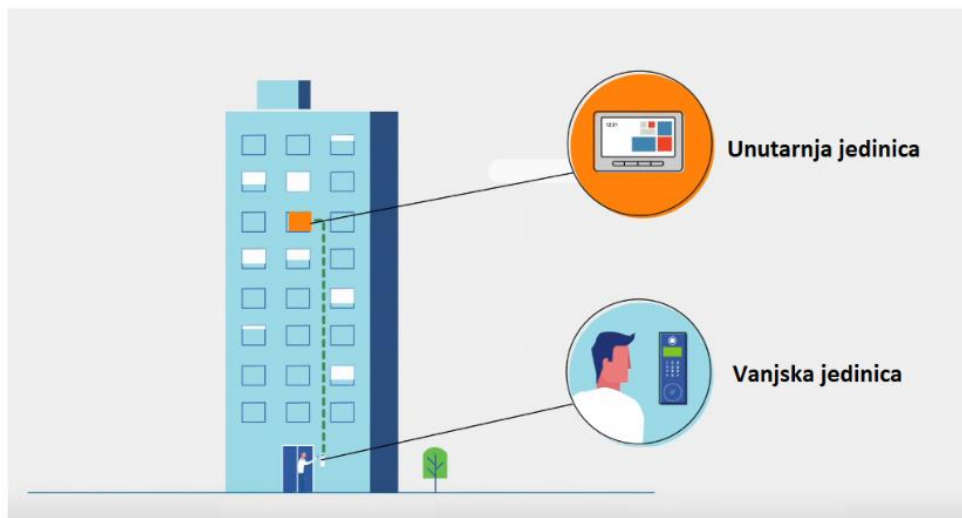
Poziv s vanjske jedinice stiže na unutarnju kao video poziv. Unutarnje jedinice imaju zaslon osjetljiv na dodir i tipku za otvaranje vrata. Povezuju se mrežnim kabelom ili bežično na lokalnu mrežnu infrastrukturu, a često ih je moguće napajati putem PoE-a. Određene jedinice nude napredne mogućnosti poput povezivanja alarmnih sustava, dodavanja i pregleda kompatibilnih IP kamera, snimanja video poziva na ugrađenu prijenosnu memoriju i druge funkcionalnosti.





4.11. *Primjer unutarnje jedinice sustava digitalne portafonije [9]*

#### 4.3.3. Način rada sustava digitalne portafonije



Slika 4.12. *Način rada sustava digitalne portafonije [9]*

Vanjska jedinica montirana je na ulazu u zgradu. Posjetitelj pozvoni na odgovarajuću tipku na vanjskoj jedinici. Poziv se upućuje prema unutarnjoj jedinici, koja vizualnim i glasovnim putem obavještava domaćina o pozivu. Pošto vanjska jedinica sadrži kameru, domaćin na unutarnjoj jedinici vidi posjetitelja te može komunicirati s njim. Ukoliko je na vanjsku portafonsku jedinicu spojen elektroprihvatnik, pritiskom na tipku na unutarnjoj jedinici domaćin može dozvoliti ulaz posjetitelju [9].

#### 4.4. Sustavi čitanja registarskih oznaka za garaže

Napredak video tehnologija, posebice videokamera i sve boljih čipova i senzora u njima otvara razne mogućnosti kada je riječ o detekcijama i nadzoru objekata i prostora. Kvaliteta visokokvalitetnih videosnimaka je postala vrhunska, te je iz njih moguće izvaditi i prepoznati vrlo sitne detalje, čak i na objektima koji se kreću velikom brzinom. Bitan podskup uporabe takvih sustava je prepoznavanje registarskih oznaka (tablica) na automobilima u pokretu ili stanju mirovanja [10].



Slika 4.13. Očitavanje registarskih oznaka [11]

Sustavi prepoznavanja tablica imaju široki spektar korištenja, od detekcije tablica automobila koji čeka dopuštenje za ulazak na zaštićeni parking (propuštaju se samo vozila s određenim tablicama – vlasnicima) do policijskog nadzora prometa kroz kamere – radare ili u patrolnim automobilima, tzv. presretačima [10].

Automatska detekcija reg.ozn. na automobilima već se dugo koristi u raznim sustavima, a posebnu primjenu ima u državnim službama. Glavni razlog za uvođenje automatske detekcije reg.ozn. je veliki porast broja automobila na cestama te olakšanje poslova koji se preciznije i brže mogu obaviti putem softverskih rješenja automatiziranih sustava.

Jedan od popularnih sustava za čitanje registarskih oznaka je i Parklio ANPR parking sustav. Ovakav sustav ima brojne prednosti [11]:

- 1) Omogućavanje automatskog pristupa ovlaštenim korisnicima - osigurava da samo ovlašteni korisnici imaju pristup parkiralištu. Potrebno je samo unijeti registarsku pločicu koju želimo dodati u sustav. Za manje od sekunde, ANPR parkirna kamera na ulazu identificira automobil s registarskom pločicom uvrštenom na popis odobrenih i dopušta ulazak podizanjem parkirne rampe. Parklio ANPR parking sustav je jedan od najbržih sustava na tržištu koji radi na svim vrstama vozila, uključujući i ona s nestandardnim registracijskim pločicama.
- 2) Nadzor i optimizacija protoka vozila – pruža mogućnosti praćenja razine popunjenosti parkirališta, te jednostavno upravljanje protokom prometa i parking kapacitetom u različito doba dana.
- 3) Ušteda vremena i novca - obavještavanje o eventualnim problemima sa sustavom, poput neispravne rampe, lančane barijere ili parking stupova. Zahtijeva minimalno održavanje. Radit će 24 sata dnevno, sedam dana u tjednu, bez ikakve intervencije.
- 4) Pruža dvosmjernu pokrivenost - dvosmjernu pokrivenost s jednom kamerom. Jedna parking rampa kontrolira ulazno-izlaznu točku parkinga te omogućuje praćenje ulazi li vozilo na parkiralište ili izlazi iz njega.
- 5) Cloud-based tehnologija - kontrola pristupa parkingu preko mobilnih telefona ili web preglednika. Automatizira i povezuje sve zadatke upravljanja parkingom u jedan objedinjeni sustav. Daje inteligentan sustav upravljanja parkingom koji se temelji na prepoznavanju registarskih tablica.
- 6) Upravljanje s više različitih lokacija putem jednog računara – upravljanje parking lokacijama s jednog računara i praćenje svih informacije o parkiralištima u stvarnom vremenu. Potrebna je samo internetska veza i računalo ili mobilni uređaj s web preglednikom za pristup računaru.
- 7) Neograničena baza podataka – moguće je staviti sve tablice klijenata u sustav. Sustav je opremljen za prepoznavanje registarskih pločica iz širokog raspona od 238 zemalja i regija, što dodatno poboljšava njegove mogućnosti i svestranost.



*Slika 4.14. Parklio ANPR parking sustav [11]*

#### **4.5. Videonadzor**

Videonadzor je sastavni dio bilo kojeg ozbiljnijeg integralnog sustava osiguranja objekta, osoba ili materijalnih dobara. Osnovna funkcija sustava video nadzora je povećanje sigurnosti i zaštite prostora i ljudi. To se postiže prevencijom kriminalnih aktivnosti kroz odvrćanje potencijalnih počinitelja, kontinuiranim praćenjem situacije u stvarnom vremenu te snimanjem i pohranjivanjem videozapisa za buduću analizu. Snimljeni materijali mogu poslužiti kao ključni dokazi u pravnim postupcima i istragama, pomažući u identifikaciji počinitelja i razjašnjavanju događaja. Osim toga, video nadzor doprinosi zaštiti zaposlenika i posjetitelja te omogućuje učinkovitu kontrolu pristupa objektima, povećavajući tako ukupnu sigurnost [12].

Projektiranje sustava video nadzora je složen proces. Projektiranje sustava video nadzora uključuje analizu sigurnosnih potreba i rizika, definiranje ciljeva sustava, odabir odgovarajuće opreme, optimalno postavljanje kamera, instalaciju kabliranja i mrežne infrastrukture, konfiguraciju softvera za upravljanje, testiranje sustava, obuku korisnika, te planiranje održavanja i nadogradnji sustava, ovdje je također vrlo bitan dio i financiranje projekta s obzirom da su cijene sustava oni što u najvećoj mjeri definira kvalitetu sustava.

#### **4.5.1. Primjena sustava videonadzora**

Moguće primjene sustava videonadzora su mnogostruke, od jednostavnih stambenih objekata pa sve do kompleksnih javnih i industrijskih objekata. Razlog je jednostavan - sustavi videonadzora dokazano dovode do smanjenja krivičnih djela (provale, krađe, vandalizma i slično) te pomažu prilikom identifikacije počinitelja. Osim toga, mogu se koristiti u svrhe nadzora proizvodnih pogona, nadzora prometa i slično. Razvojem novih tehnologija i mogućnostima integracije sustava videonadzora s ostalim sustavima primjene su gotovo neograničene.

#### **4.5.2. Komponente sustava videonadzora**

Sustavi videonadzora mogu biti iznimno kompleksni. Također, ovisno da li se radi o analognom ili digitalnom sustavu videonadzora, različite su i komponente samoga sustava i material tih komponenti. Međutim, manje-više se svaki sustav sastoji od sljedećih komponenti:

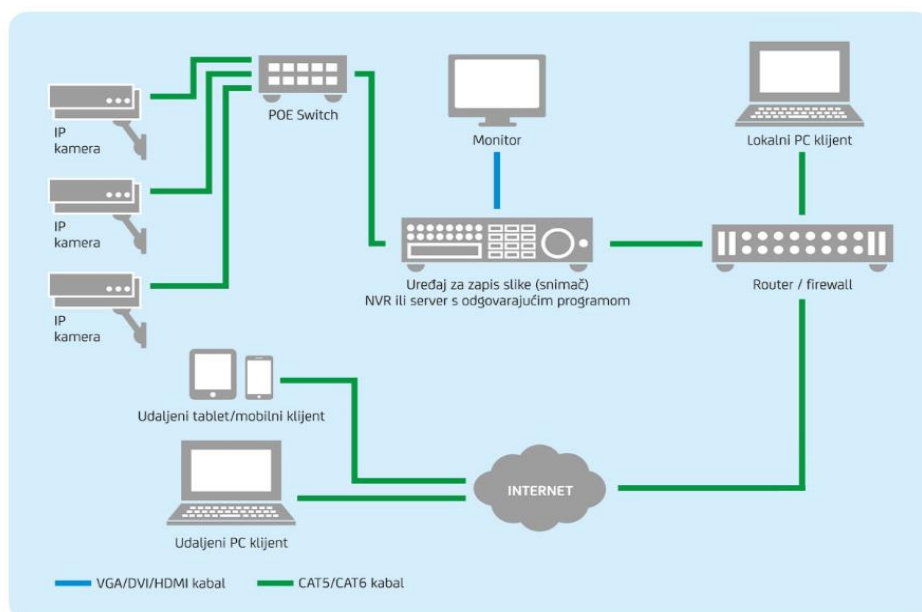
- 1) Kamera - za snimanje slike i videozapisa potrebna je video kamera. Danas se obično koriste IP kamere za potrebe video nadzora, ali za puno sustava se i dalje koriste analogne kamere i snimači.
- 2) Kablovi - putem kablova se slika koju je snimila kamera šalje do snimača. Za IP kamere se koriste UTP kablovi, za analogne koaksijalni.
- 3) Snimači - snimač prima snimljeni video sa kamere te ga sprema na disk i prikazuje ga na spojeni monitor. Tzv. mrežnim snimačima moguće je pristupiti i putem mreže te vršiti pregled uživo ili pregled snimljenog materijala sa računala ili mobitela.
- 4) Napajanje - za napajanje analognih kamera obično se koristi 12 VDC ispravljač. IP kamere najčešće podržavaju PoE te imaju mogućnost da ih se napaja putem mreže, ukoliko switch ili snimač ima na sebi PoE portove.
- 5) Mrežni uređaji – pošto IP kamere i mrežni snimači koriste TCP/IP protokole za prijenos signala, za međusobnu komunikaciju potrebna je računalna mreža te uređaji poput routera i switcheva. Obično je postojeća računalna

mreža i više nego dovoljna da podrži sustave videonadzora manje do srednje veličine.

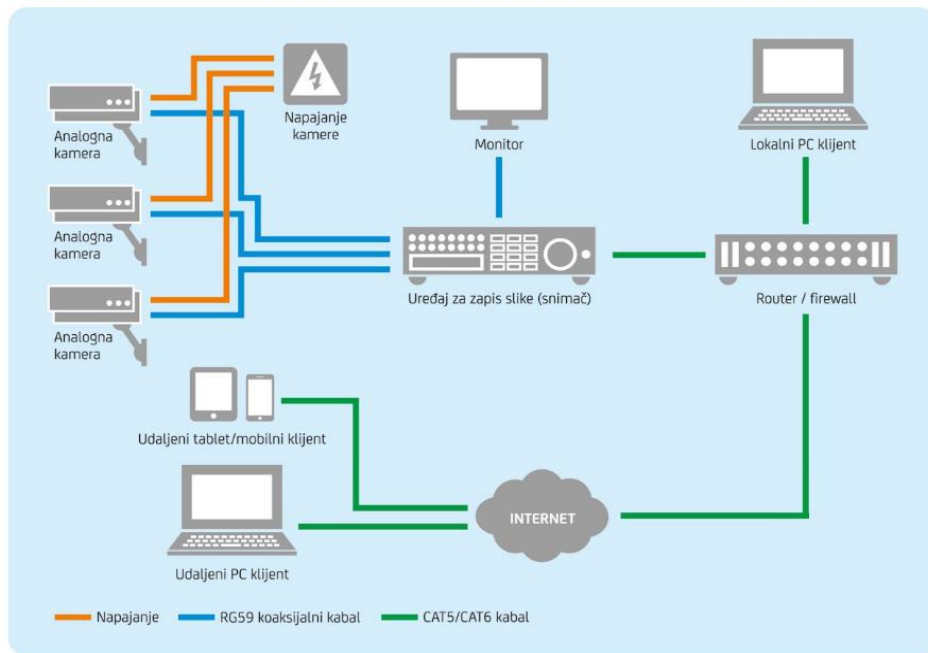
- 6) Računalo sa video softverom - na računalo klijenta obično se instalira softver za pregled i upravljanje video nadzorom. Softver ovog tipa omogućuje prikaz videa uživo, pregled snimljenog materijala, upravljanje kamerama i snimačima. Mnogi proizvođači danas nude i pregled snimke putem aplikacije na mobilnom telefonu.

#### 4.5.3. Grafički prikaz sustava videonadzora

Kao što je rečeno, postoje analogni i digitalni sustavi videonadzora. Analogni sustavi ne koriste lokalnu mrežu za povezivanje kamera i snimača i obično zahtijevaju dodatno napajanje za svaku kameru. Sljedećim prikazima dane su sheme analognog i digitalnog sustava videonadzora.



Slika 4.15. Grafički prikaz digitalnog sustava videonadzora [7]



Slika 4.16. Grafički prikaz analognog sustava videonadzora [7]

#### 4.5.4. Tipovi kamera

Kamere se najčešće dijele po obliku tijela kamere pa tako imamo:

- 1) Box kamere - kamere koje dolaze bez objektiva. Ove kamere zahtijevaju kupovinu objektiva kao i nosača na koji će biti montirane.



Slika 4.17. Box kamera [7]

2) Bullet kamere - kamere koje se nalaze u cjevastom kućištu.



*Slika 4.18. Bullet kamera [7]*

3) Dome kamere - kamere koje se nalaze u kućištu u obliku polukugle.



*Slika 4.19. Dome kamera [7]*

4) PTZ kamere - pomične kamere koje je moguće softverski rotirati.



*Slika 4.20. PTZ kamera [7]*

Osim to tijelu kamere, kamere se razlikuju i po rezoluciji, žarišnoj duljini objektivna (određuje vidni kut kamere), stupnju IP zaštite, podršci za IR, WDR itd.



#### 4.5.5. Tipovi snimača

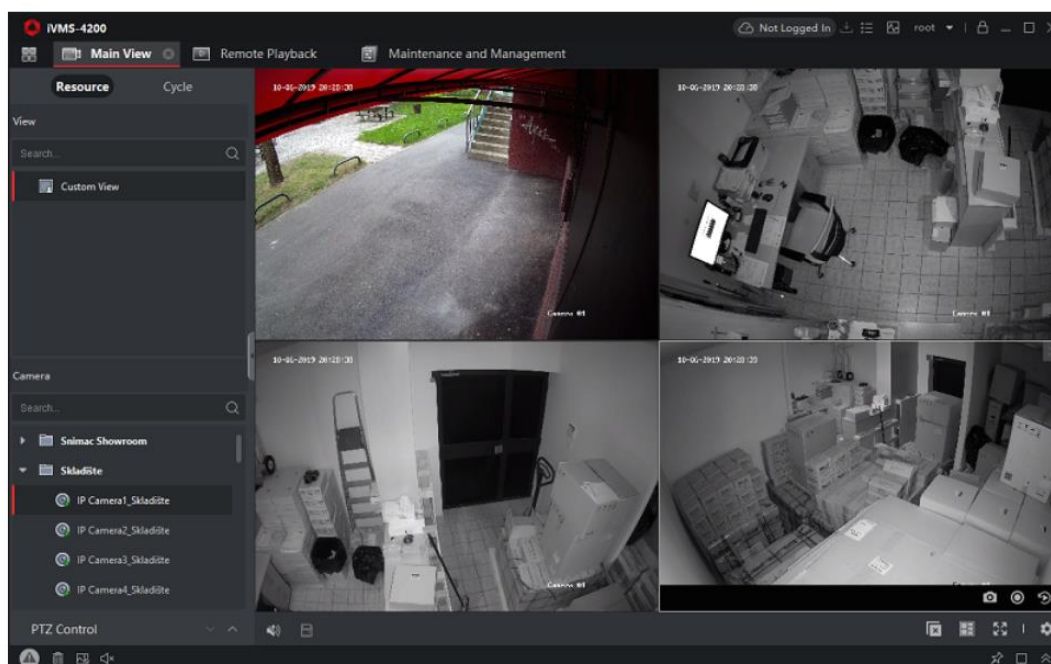
Snimači se obično dijele po broju kamera koje se mogu spojiti na njih. Imamo 4-kanalne, 8-kanalne, 16-kanalne, pa sve do 256-kanalne snimače. Bitno je još je pripaziti na podržanu rezoluciju snimanja, ulazni i dolazni mrežni bandwidth, izlaze za monitore (VGA, HDMI, CVBS), alarmne ulaze i izlaze.



Slika 4.21. Analogni (lijevo) i digitalni (desno) snimač [7]

#### 4.5.6. Softver

Klijentski softver omogućuje istovremeno spajanje na više različitih snimača s jednog klijent računala.[13]. Klijentski softver obično se instalira na isto računalo i snimač unutar mreže. Koristi se za praćenje prijenosa uživo, pregled snimljenog materijala, izvlačenje snimki i konfiguraciju sustava videonadzora.



Slika 4.22. Softver za sustav videonadzora [7]

## **4.6. Protuprovalni sustav**

Porastom krađa i provala javlja se veća potreba za ugradnjom sustava tehničke zaštite koji nas upozoravaju da je štićeni objekt ili prostor ugrožen djelovanjem nekog trećeg lica. Kako provalnici često idu linijom manjeg otpora, ugradnja vidljivih znakova ugrađenog protuprovalnog sustava (sirene, bljeskalice, vanjski detektori) će ih najčešće odvratiti od provale, krađe ili devastacije štićenog prostora. Pravovremena informacija ili upozorenje protuprovalnog sustava znatno umanjuje mogućnost otuđenja stvari ili devastacije štićenog prostora [14].

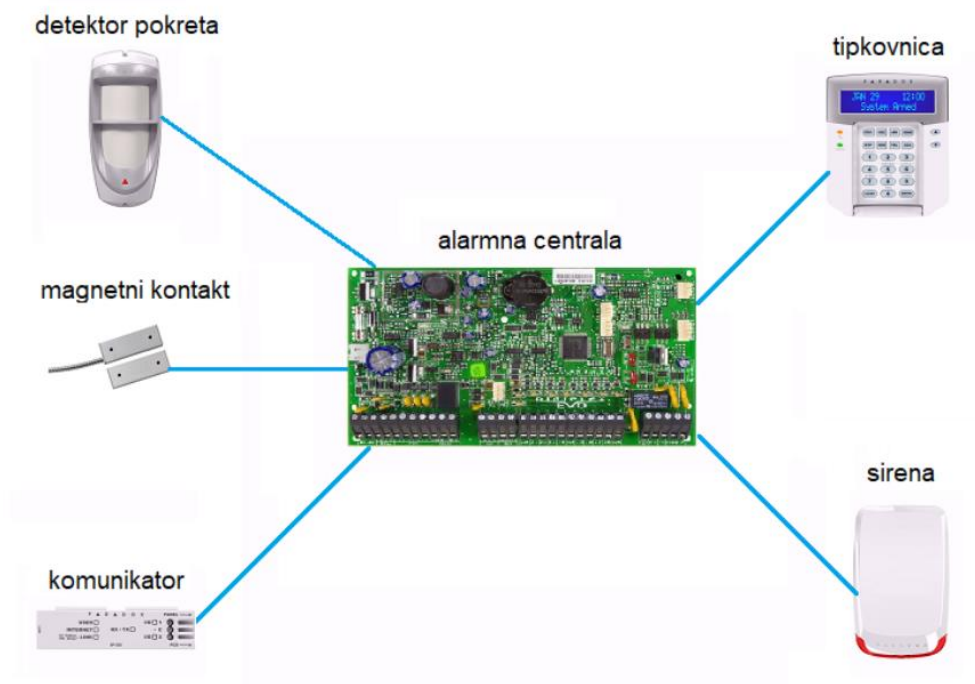
Protuprovalni tehnički sustavi se sastoje od nekoliko ključnih elemenata. To su alarmna centrala, uređaji za upravljanje poput tipkovnica ili druge vrste periferije i modula proširenja, detektori za unutarnju ili vanjsku upotrebu i za detekciju stanja okoline, komunikacijski uređaji kao što su glasovni dojavnici, GSM, GPRS i TCP/IP komunikatori, te signalizacija za vanjsku ili unutarnju primjenu koja uzbuđuje kako korisnike tako i relevantne službe.

### **4.6.1. Signalizacija**

Može biti zvučna (sirene) ili svjetlosna (bljeskalice). Služi za lokalno uzbuđivanje u slučaju povrede sigurnosnog stanja objekta.

### **4.6.2. Način rada protuprovalnog sustava**

Sljedeća slika daje grafički prikaz alarmnog sustava, elemente od kojih se sustav sastoji te način na koji se elementi spojeni.



Slika 4.23. Alarmni protuprovalni sustav [14]

Sve komponente alarmnog sustava se spajaju na alarmnu centralu. Tipkovnica služi za uključivanje i isključivanje sustava. Detektori pokreta i magnetni kontakti otkrivaju upad u štice prostora te šalju tu informaciju centrali. Sirena služi za lokalno uzbunjivanje i oglašava se u slučaju alarma. Komunikator dojavljuje informaciju o povredi sigurnosnog stanja objekta na privatni mobitel korisnika ili na dojavni centar. Također, moguće je ostvariti i bežični sustav. Bežični sustav pravo je rješenje gdje god građevinski radovi nisu mogući ili se želi uštedjeti na vremenu potrebnom za instalaciju sustava [14].

#### 4.7. Sustavi vatrodjave

Sustavi vatrodjave ključni su za rano otkrivanje požara i sprečavanje njegovog širenja, osiguravajući sigurnost ljudi i imovine. Projektiranje i implementacija sustava vatrodjave uključuje nekoliko važnih aspekata:

**Detektori požara:** Postoje različite vrste detektora, uključujući detektore dima, topline, plamena i plinova. Svaki od ovih detektora dizajniran je za specifične uvjete i vrste požara. Detektori dima najčešće se koriste za rano otkrivanje, dok detektori topline reagiraju na porast temperature. Centralna upravljačka jedinica:

Ovo je srce sustava vatrodajave. Centralna upravljačka jedinica (Centrale) prima signale od detektora i aktivira alarme. Također može biti povezana s drugim sigurnosnim sustavima, kao što su sustavi za automatsko gašenje požara, ventilacija i evakuacijski sustavi. Alarmni sustavi: Alarmni uređaji, uključujući zvučne i svjetlosne signale, upozoravaju osobe u zgradi na opasnost od požara. Ovi alarmi moraju biti dovoljno glasni i vidljivi kako bi osigurali da svi budu pravovremeno obaviješteni. Ručni javljači požara: Ručni javljači požara (tipke za alarm) omogućuju ljudima da ručno aktiviraju alarm u slučaju požara. Oni su obično postavljeni na strateškim mjestima u zgradi, kao što su izlazi i hodnici. Integracija s drugim sustavima: Sustavi vatrodajave često su integrirani s drugim sigurnosnim sustavima, kao što su sustavi za automatsko gašenje požara (npr. sprinkler sustavi), sustavi za kontrolu pristupa i evakuacijski sustavi. Ovo omogućuje koordiniranu reakciju na požar. Redovito održavanje i testiranje: Kako bi sustav vatrodajave bio učinkovit, potrebno ga je redovito održavati i testirati. To uključuje provjeru detektora, testiranje alarma i osiguravanje da su sve komponente sustava u ispravnom stanju. Poštivanje standarda i propisa: Projektiranje i instalacija sustava vatrodajave moraju biti u skladu s nacionalnim i međunarodnim standardima i propisima. Ovo uključuje propise o protupožarnoj zaštiti i sigurnosne standarde.

#### **4.7.1. Komponente vatrodajavnog sustava**

Sustav vatrodajave mogu biti donekle različiti no svi imaju istu osnovu i sastoje se od sljedećih komponenti:

Upravljačka centrala: To je "glavni mozak" sustava koji prima signale od detektora, obrađuje podatke te vrši aktivacije alarma ili izvršnih funkcija.

Detektori dima, para, aerosola, maglica: Otkrivaju prisutnost navedenih medija koji su indikatori gorenja.

Detektori topline: Reagiraju na povećanje temperature ili na izmjene temperature u određenom parametru.

Ručni javljači (aktivatori alarma): Omogućuju korisnicima da ručno aktiviraju alarme

Sirene: Aktivacija i odašiljanje zvučnog signala za uzbunjivanje ljudi.

Bljeskalice: Vizualni signali za uzbunjivanje korisnika.

Svjetlosni pokazivači / indikatori: Pokazuju lokaciju požara unutar zgrade.

Bežični prijenosnici signala: Omogućuju bežičnu komunikaciju između komponenti.

Napajanje (baterije, napajanje iz mreže): Osigurava se rad sustava, čak i u slučaju nestanka struje, sustavi se prebacuju na "backup".

Moduli za gašenje: Aktiviraju sustave za automatsko gašenje požara (npr. sprinkler sustave ili stabilne sustave za gašenje požara).

Komunikacijski moduli: Povezuju sustav s vanjskim nadzornim centrima ili drugim sustavima zaštite, također ih se može spojiti sa službama sigurnosti ili vatrogasnim postajama.

Releji i prekidači: Upravlja napajanjem i povezivanjem različitih dijelova sustava.

Sustavi za nadzor i upravljanje: Omogućava praćenje i upravljanje rada sustava.

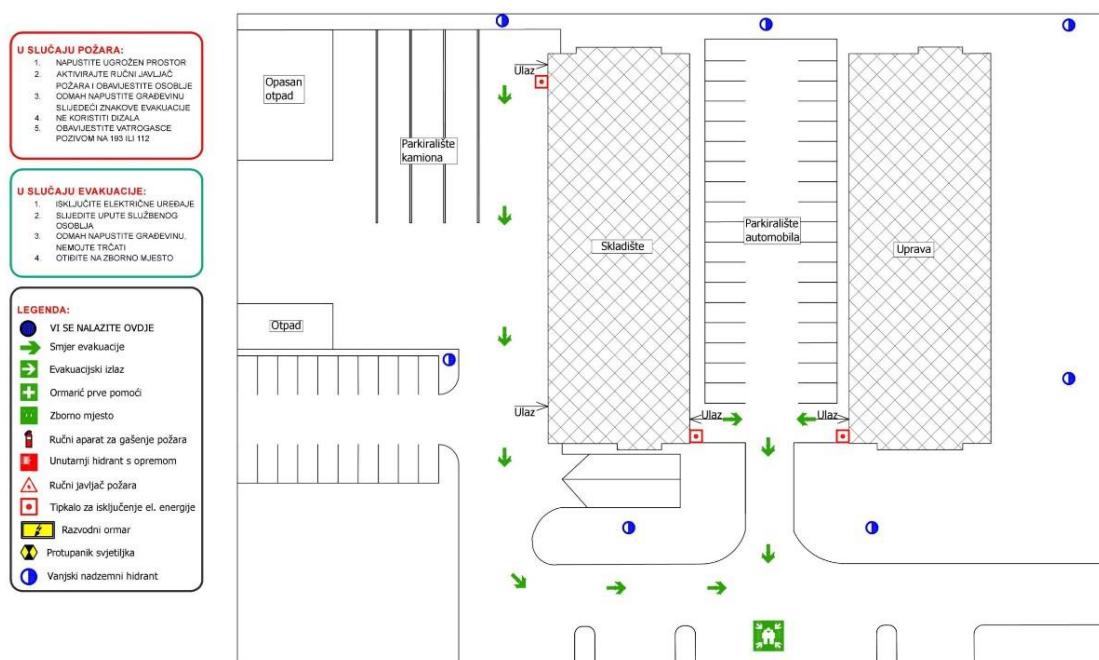
#### **4.8. Sustavi evakuacije**

Evakuacija podrazumijeva organizirano napuštanje mjesta rada odnosno ugroženog područja od strane radnika i drugih osoba u slučaju kada za njihov život ili zdravlje nastupi ili može nastupiti opasnost zbog izvanrednog događaja ili kada takav događaj može imati za posljedicu materijalnu štetu većeg opsega [17]. Plan evakuacije i spašavanja kod poslodavca podrazumijeva izradu istoimenog dokumenta u kojem je potrebno navesti i obraditi sve bitne elemente koji mogu utjecati na nastanak izvanrednog događaja, kao i uspješno provođenje evakuacije i spašavanja [17].

Plan evakuacije se sastoji od tekstualnog i grafičkog dijela. Tekstualni dio plana podrazumijeva obrađivanje svih važnih sastavnica koje bi mogle uvjetovati ili utjecati na uspješno provođenje evakuacije i spašavanje iz radnih prostorija poslodavca. Grafički dio plana bi trebao obuhvaćati sljedeće elemente [17]:

- prikaz situacije objekta na koji se plan odnosi u odnosu na druge okolne objekte,

- prikaz tlocrta svih etaža u sklopu objekta na koji se plan odnosi te smjerova evakuacije,
- prikaz evakuacijskih izlaza,
- prikaz tehničkih sustava i opreme za evakuaciju i spašavanje,
- prikaz unutrašnjih i vanjski evakuacijskih putova,
- prikaz sigurnih mjesta okupljanja nakon evakuacije,
- prikaz pozicija opasnih sadržaja i drugo.



Slika 4.24. Evakuacijski plan [17]

Osnovna namjena elektroničkog sustava evakuacije je upravljanje i nadziranje evakuacijskim prolazima (jedno krilna zaokretna vrata ili dvokrilna zaokretna vrata) sa ciljem konstantnog nadzora nad statusom vrata (vrata otvorena, vrata zatvorena, vrata zaključana, vrata pritvorena i dr.) te jednostavnog otvaranja vrata u slučaju nužde (vatra, potres i sl.). Sustav evakuacije sastoji se od evakuacijskog terminala, elektromagnetske panik brave ili mehaničke panik brave i evakuacijskog elektromagnetskog prihvatnika, centralne nadzorno-upravljačke jedinice i instalacija [18].



*Slika 4.25. Evakuacijski terminal [18]*

#### **4.9. Sustavi hidrantskih mreža za gašenje požara**

Hidrantska mreža za gašenje požara je skup cjevovoda, uređaja i opreme kojima se voda od izvora dovodi do štíćenih prostora i građevina. Za zaštitu objekata projektiraju se i izvode unutarnje hidrantske mreže [19]. Vanjska hidrantska mreža za gašenje požara je hidrantska mreža za gašenje požara izvedena izvan građevine koja se štiti, a završava nadzemnim ili podzemnim hidrantom [20].

##### **4.9.1. Unutarnja hidrantska mreža**

Hidrantska mreža unutarnjeg tipa mora biti izvedena na način da u potpunosti prekriva štíćeni prostora najmanje jednim mlazom vode. U zgradi koja se štiti unutarnjom hidrantskom mrežom za gašenje požara postavljaju se zidni hidranti na cjevovod, a oni moraju biti postavljeni tako da omogućuju sigurno i učinkovito rukovanje i upotrebu, moraju biti dostupni i pravilno označeni.



*Slika 4.26. Zidni hidrantski ormar [20]*

Unutrašnja hidrantska mreža izvodi se kao mokra i suha. Suhu hidrantsku mrežu danas najčešće susrećemo u javnim otvorenim, poluotvorenim i podzemnim garažama koje nisu grijane, ili u industrijskim pogonima koji su poluotvorenog ili otvorenog tipa i gdje grijanje prostora nije moguće, a hidrantska mreža je neophodna. Suha hidrantska mreža izvodi se isto kao i mokra hidrantska mreža s klasičnim hidrantskim ormarićima. Jedina razlika između suhe hidrantske mreže i mokre hidrantske mreže je uvjet da se svi cjevovodi suhe hidrantske mreže moraju moći potpuno isprazniti (drenirati) poslije upotrebe ili poslije probe pod pritiskom [19].



Unutarnjom hidrantskom mrežom za gašenje požara moraju se štititi [20]:

- građevine i prostori za koje je to traženo posebnim propisima,
- građevine i prostori za koje je to traženo posebnim uvjetima građenja iz područja zaštite od požara,
- građevine za koje je to zahtijevano prostornim planom,
- građevine koje svojim značajkama spadaju u I., II. ili III. kategoriju ugroženosti od požara sukladno odredbama Pravilnika o razvrstavanju građevina, građevinskih dijelova i prostora u kategorije ugroženosti od požara,
- objekti čija je kota poda najviše etaže namijenjene za boravak ljudi najmanje 9 m iznad najniže kote površine uz stambeni objekt koja služi kao vatrogasni pristup,
- mjesta okupljanja većeg broja ljudi u građevinama,
- garaže i parkirališta u građevinama, čija je površina veća od 100 m<sup>2</sup>,
- građevine i prostori namijenjeni trgovini čija je površina veća od 100 m<sup>2</sup>,
- podzemne etaže površine veće od 100 m<sup>2</sup> i
- mjesta stalnog zavarivanja koja se nalaze unutar građevine.

#### **4.9.2. Vanjska hidrantska mreža**

Vanjska hidrantska mreža za gašenje požara je hidrantska mreža za gašenje požara izvedena izvan građevine koja se štiti, a završava nadzemnim ili podzemnim hidrantom [20]. Vanjska hidrantska mreža za gašenje požara mora imati siguran izvor vode takvog kapaciteta da omogući opskrbu minimalno propisanom protočnom količinom vode koja je potrebna za zaštitu požarnog sektora s najvećim požarnim opterećenjem građevine koja se štiti, uz tlak na hidrantu koji nije manji od tlaka koji je propisan u trajanju od najmanje 120 minuta [20].



*Slika 4.27. Sustav vanjske hidrantske mreže [21]*

Vanjskom hidrantskom mrežom za gašenje požara obvezatno se moraju štiti [20]:

- građevine i prostori za koje je to traženo posebnim propisima,
- građevine i prostori za koje je to traženo posebnim uvjetima građenja iz područja zaštite od požara,
- građevine i prostori za koje je to zahtijevano prostornim planom,
- naseljena mjesta koja imaju izgrađen vodoopskrbni sustav i
- građevine i prostori koji svojim značajkama spadaju u I., II. ili III. kategoriju ugroženosti od požara, izuzev prostora sa zaštićenom i visokokvalitetnom šumom (nacionalni parkovi i sl.) za koje će se moguća obveza izgradnje hidrantske mreže utvrditi u procjeni ugroženosti od požara.

#### **4.10. Stabilni sustavi gašenja**

Stabilni sustavi za gašenje požara su sustavi koji su dizajnirani da se koriste za gašenje požara u ranim fazama, prije nego što postanu preveliki i prije nego što se požar proširi na druge dijelove objekta. Ovi sustavi su obično instalirani u područjima s povećanim rizikom od požara, kao što su kuhinje, kemijski laboratoriji, spremišta s gorivom i drugi slični prostori. Stabilni sustavi za gašenje požara koriste se obično u kombinaciji s drugim sustavima za dojavu požara kako bi se postigla što brža reakcija u slučaju pojave požara. Ovi sustavi

se razlikuju od klasičnih sustava za gašenje požara jer su dizajnirani za gašenje požara u ranim fazama i brzo reagiraju na izvor požara [22]. Stabilni sustavi za gašenje požara se mogu podijeliti na plinske sustave, sustavi za gašenje vodom, sustavi za gašenje pjenom, sustavi za gašenje prahom i sustavi za gašenje kemikalijama [22]. Neki od općih elemenata stabilnih sustava za gašenje požara su spremnik sredstva za gašenje požara, cjevovodni sustav, pumpe, uređaj za aktivaciju ili aktivatori, raspršivači, električni ormari, signalni uređaji.

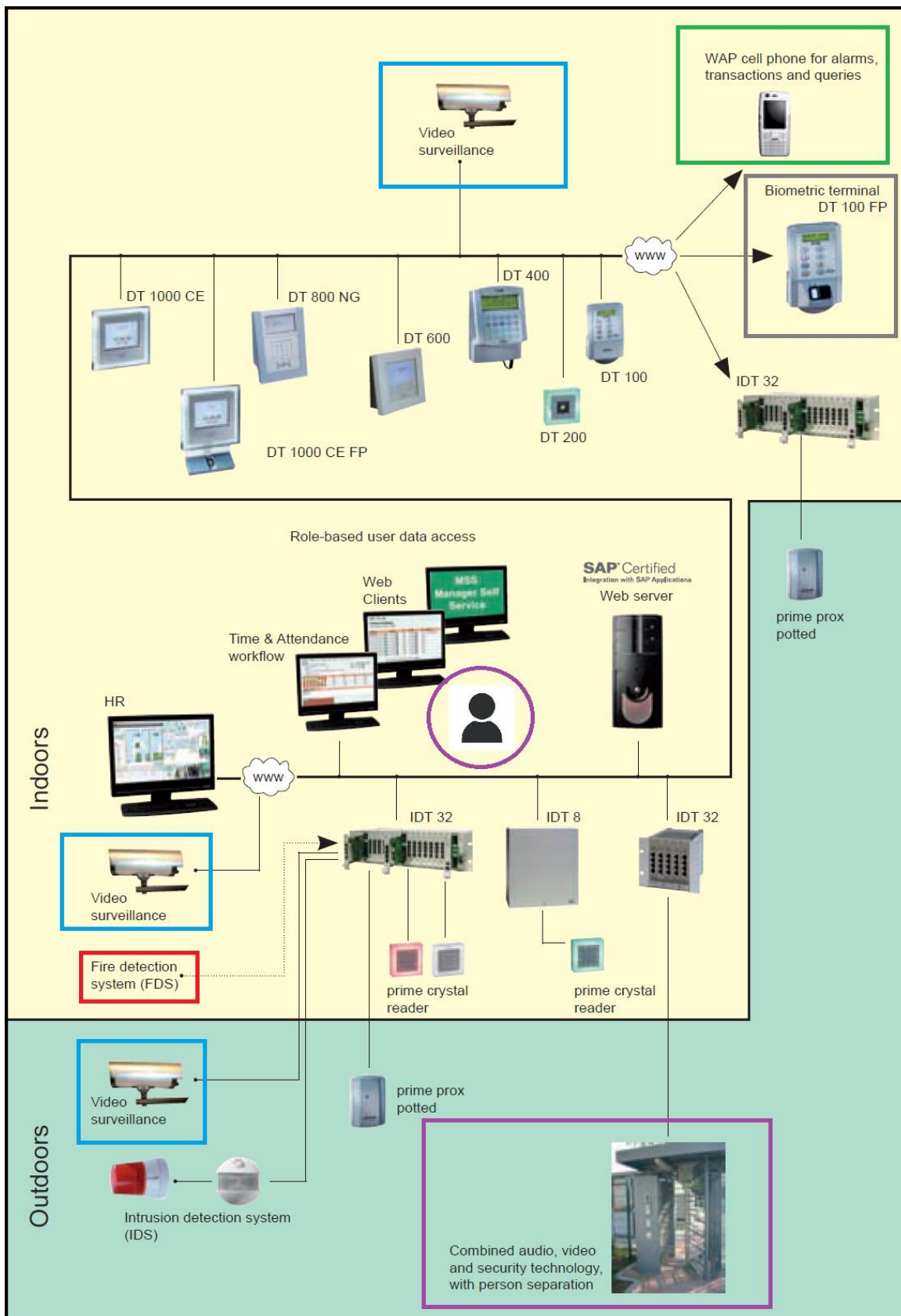
Tablica 4.1. Podjela stabilnih sustava za gašenje požara [22]

<b>Vrsta sustava</b>	<b>Primjena</b>	<b>Podjela</b>
Plinski sustavi	Industrija, komercijalni i stambeni objekti	Inertni plinovi (npr. argon, dušik)
		Ugljični dioksid (CO <sub>2</sub> )
Sustavi za gašenje vodom	Komercijalni i stambeni objekti	Sustavi za gašenje popratnih požara
		Sustavi za gašenje požara na otvorenom prostoru
Sustavi za gašenje pjenom	Rafinerije, zrakoplovne i pomorske industrije	Sustavi za gašenje velikih industrijskih požara
		Sustavi za gašenje požara na brodovima i platformama
Sustavi za gašenje prahom	Skladišta, zrakoplovne i pomorske industrije	Sustavi za gašenje požara u procesima praškastih materijala
		Sustavi za gašenje požara u zrakoplovima i na brodovima
Sustavi za gašenje kemikalijama	Procesne industrije, laboratoriji	Sustavi za gašenje požara uzrokovanih kemikalijama

## 5. INTEGRACIJA

Integracija je ključna riječ kad je u pitanju rad sigurnosnih sustava. U različitim industrijama koriste se različiti sustavi te ovisno o potrebnoj razini sigurnosti odabiru se sustavi sigurnosti. Kako ljudi žive u sve većim zajednicama u zgradama ili kompleksima zgrada i tu su se počeli implementirati sustavi sigurnosti i zaštite no primarno se i dalje koriste u industriji. Sustavi se prvo odvojeno instaliraju nakon čega se povezuju u mreže sa prosljeđivanjem informacija i aktivacijama određenih funkcija koje su ovisne o uzroku aktivacije. Najnovije tehnologije koriste umjetnu inteligenciju za poboljšavanje rada, dronove, kamere visoke razlučivosti, IR, UV, termo i druge vrste senzora za detekciju opasnosti. Kamere za prepoznavanje lica su rasprostranjene u uporabi te prepoznaju lica s velikom razinom točnosti. Sustavi sigurnosti se također povezuju i sa drugim sustavima (ventilacije, hlađenja, klime i sl.) u proizvodnim pogonima da bi se kontroliralo nastajanje štete, da bi se zaštitili ljudi i proizvodi. Za ovo je dobar primjer povezivanje sustava vatrodojave sa tzv. HVAC sustavima koji se isključuju pri aktivaciji vatrodojave da bi se spriječilo širenje požara u slučaju nastanka. U zgradama kao što su trgovački centri izvršne funkcije su drugačije naravi zbog velikog broja posjetitelja i drugačije naravi objekta, tamo se zaustavljaju pokretne stepenice, liftovi odlaze u početnu poziciju/kat te ih se više ne može koristiti (osim liftova za vatrogasce) aktivira se odaljšavanje prostora itd. Ideja koja se naziva u suštini integracije je da sustavi obavljaju funkcije koje štite korisnike na način da oni ne trebaju imati znanje o radu sustava. Sustavi se programiraju unaprijed i obavljaju funkcije koje su im zadane. Kontrola pristupa se integrira s sustavom protuprovala na način da korisnici mogu ući u određene prostore a kad je radno vrijeme gotovo dolazi do uključivanja protuprovala na način da se pri ulasku u prostore oglašavaju alarmi, sustav video nadzora se spaja na protuprovala te se snimanje kamerama aktivira zbog ulaska izvan radnog vremena. Na ove sustave se nadovezuje sustav vatrodojave koji ima mogućnost deaktivacije kontrole pristupa da se može obaviti evakuacija po potrebi. Na sustav vatrodojave se povezuju sustavi stabilnog gašenja koji se mogu aktivirati u slučaju izbijanja požara, požar također može biti detektiran i kamerama koje su za to

namijenjene. Primjera integracije tehničkih sustava sigurnosti je sve više no treba imati na umu da je ključan faktor upravljanje sustavima, dakle potrebno je da djelatnici službe sigurnosti znaju reagirati u slučaju aktivacije sustava i da se izbjegnu zlouporabe no također da se izbjegne nepotrebno dugi period aktivacije sustava jer sustavi sigurnosti onemogućuju rad drugih sustava na koje su povezani a druge strane aktiviraju sirene i druge pripadajuće izvršne funkcije. Korištenje tehničkih sustava sigurnosti i njihova integracija je smjer u kojem se razvija politika sigurnosti velikih kompanija i cijelog društva općenito jer je Sigurnost osnovni preduvjet za nesmetan rad i ugodan život.



Slika 5.1. Block dijagram integracija tehničkih sustava sigurnosti [10]

## 5.1. Kontrola pristupa i evidencije radnog vremena

Sustav kontrole pristupa se često povezuje s evidencijom radnog vremena jer su sustavi logično povezani u smislu medija identifikacije i pozicije čitača. Čitač koji se koristi za kontrolu pristupa moguće je iskoristiti i za kontrolu radnog vremena te je iz istog softvera moguće vršiti upravljanje oba sustava.



Slika 5.2. Kontrola pristupa i evidencije radnog vremena [25]

## 5.2. Centralni dojavni sustav

Centralni dojavni sustav (CDS) - informacija o promjeni stanja alarmnog sustava se šalje na odabrani Centralni dojavni sustav. Osnovna svrha Centralnog dojavnog sustava je mogućnost primanja informacija koje šalju alarmni sustavi, analiza i obrada primljenih podataka te pohrana istih. U slučaju alarma, dežurni operater na dojavnom centru postupa po unaprijed definiranoj proceduri (npr. poziv vlasniku štíćenog prostora, alarmiranje sigurnosnih službi, slanje interventnih ekipa zaštitarski službi, itd.). U slučaju da se kontakt ne može ostvariti, na objekt se šalju zaštitari koji imaju zadatak utvrditi provjeru sigurnosnog stanja štíćenog objekta.

### **5.3. Sustav digitalne portafonije**

- mogućnost spajanja alarmnih uređaja na unutarnju jedinicu (npr. detektora ugljičnog monoksida ili vatrodojavnog detektora)

### **5.4. Videonadzor i vatrodojava**

Požare otvorenog prostora, obzirom na velike površine koje treba štiti, nije moguće detektirati klasičnim metodama detekcije koje se primjenjuju u zatvorenim prostorima te se u tu svrhu koriste sustavi videonadzora.

Sastoje se od pokretnih kamera s velikom mogućnošću povećavanja (tzv. zoom-a) koje se instaliraju na uzvišenim lokacijama s kojih se dobro vide okolne površine pokrivene šumom ili drugim raslinjem te poljoprivredna zemljišta. Kamere se bežičnom vezom povezuju u centar u kojem dežurni vatrogasac može na monitoru promatrati slike iz nadziranih područja. Ovisno o veličini područja koje se štiti, moguće je tako nadzirati i desetke kamera pa jedan čovjek u centru može nadzirati veliko zemljopisno područje. Kamere se obično postavljaju da automatski kruže programiranom rutom, a u slučaju da primijeti sumnjivi dim ili plamen, dežurni vatrogasac može preuzeti kontrolu nad kamerom i po potrebi povećati taj dio slike kako bi se uvjerio u postojanje požara i obavijestio vatrogasce. Osim promatranja operatera, koriste se i specijalni softveri za zaštitu od požara koji u slici primljenoj putem kamera detektiraju spektar karakterističan za plamen te upozoravaju operatera. Primjer primjene videonadzora u zaštiti otvorenog prostora od požara s posebnim softverom, razvijenim na splitskom Fakultetu strojarstva, brodogradnje i elektrotehnike pod vodstvom prof. Darka Stipaničeva, je i sustav izveden za zaštitu Nacionalnog parka Paklenica. Protuprovalne sustave moguće je proširiti detektorima plamena, dima ili plina tako da nas ista alarmna centrala alarmira pri povećanju njihove koncentracije u zraku.

### **5.5. Vatrodojava i protuprovala**

U mnogim objektima ekonomično je sustav dojava požara kombinirati sa sustavom protuprovala i koristiti istu alarmnu centralu. Vlasnici objekata često



sustav za dojavu požara zahtijevaju kada su objekti već u upotrebi. Kako bi se izbjegle dodatne građevinske intervencije praktičnije je koristiti bežične vatrodojavne detektore umjesto žičanih. Prednost korištenja bežičnih detektora je i lokalna signalizacija jer svaki od njih ima ugradbenu zujalicu. Osim potrebe za zaštitom od požara, raste i potreba za zaštitom od nesreća uzrokovanih istjecanjem gradskog plina i trovanja ugljičnim monoksidom zbog neispravnih dimnjaka. Kako bi se i takve opasnosti spriječile ili barem smanjile preporučljivo je u stambeni prostor ugraditi detektor plina i/ili ugljičnog monoksida i spojiti ga na već postojeću protuprovalno -vatrodojavnu centralu. Ukoliko u objektu ne postoji sustav protuprovale i korisnik ne želi centralizirani nadzor moguće je dojavu požara i plina izvesti i nezavisnim vatrodojavnim detektorima koji tada samo lokalno signaliziraju alarm bez aktiviranja sirena za uzbunjivanje okolice i pozivanja intervencije.

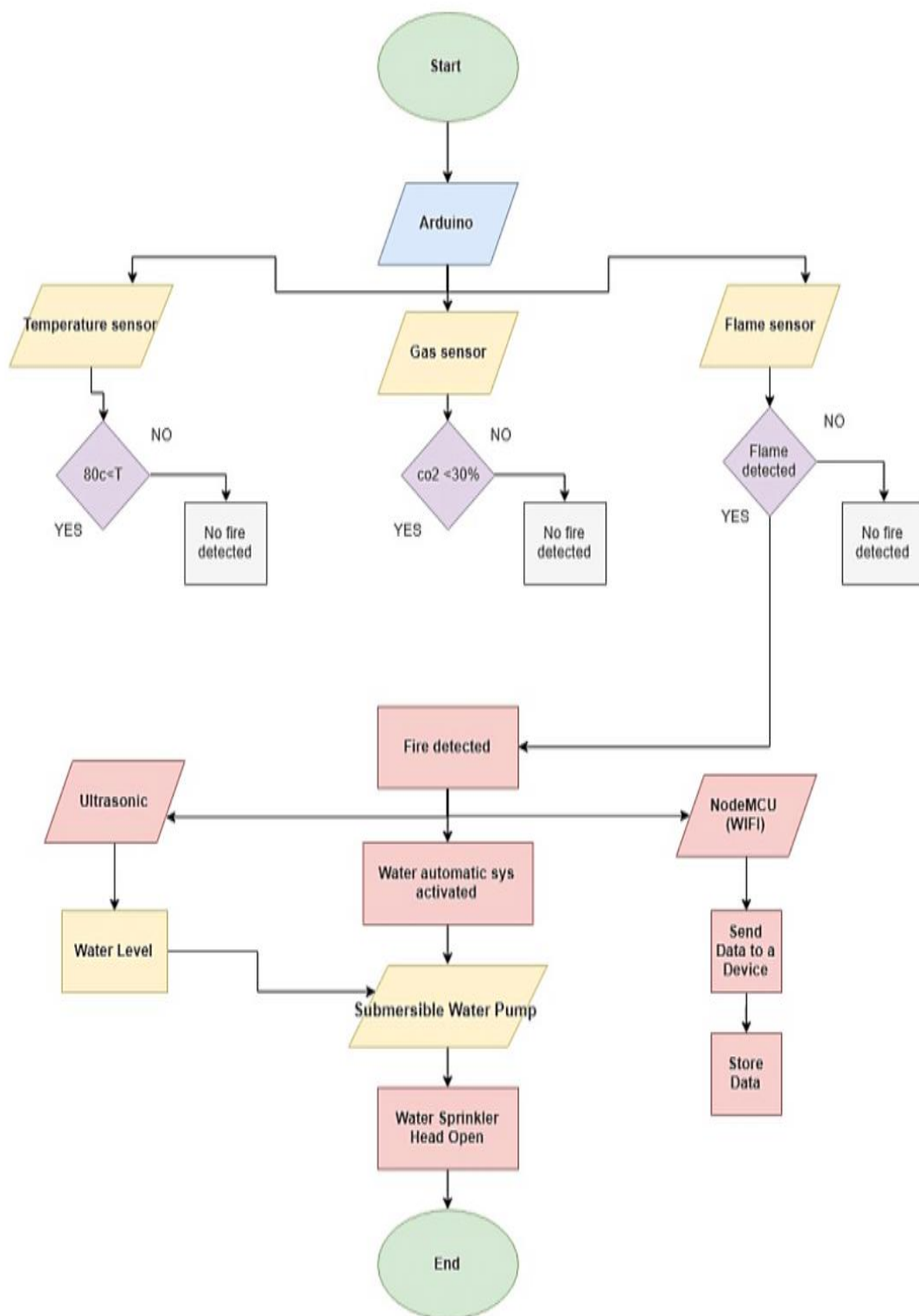
Moguće je integrirati javljače požara sa postojećim protuprovalnim sustavom.

## **5.6. Sprinkleri, vatrodojava i gašenje požara**

Integracija sprinkler sustava s vatrodojavom omogućuje automatsko gašenje požara kroz koordiniranu detekciju i odgovor na pojavu požara. Kada senzori vatrodojavnog sustava, poput detektora dima, topline ili plamena, otkriju požar, oni šalju signal centralnoj upravljačkoj jedinici. Centralna upravljačka jedinica obrađuje ove signale i, ako su zadovoljeni određeni kriteriji, aktivira ventil sprinkler sustava. Ovaj ventil omogućuje protok vode kroz cijevi do raspršivača, koji raspršuju vodu po zahvaćenom području, čime se požar automatski gasi. Elektronska integracija između sustava vatrodojave i sprinkler sustava obavlja se pomoću releja i kontrolnih ploča koje upravljaju otvaranjem ventila. Signal iz sustava vatrodojave osigurava pravovremenu aktivaciju sprinklera, što omogućuje brzu reakciju i učinkovito gašenje požara. Osim toga, sustav vatrodojave i sprinkler sustav mogu raditi u sinergiji kako bi osigurali maksimalnu zaštitu. Na primjer, dok detektori dima ili topline u sustavu vatrodojave otkriju početnu fazu požara i aktiviraju sprinkler sustav, istovremeno se aktiviraju i zvučni i svjetlosni alarmi koji upozoravaju ljude u zgradi, omogućujući im brzu evakuaciju.

U slučajevima kada se sustav vatrodojave i sprinkler sustav koriste zajedno, automatsko gašenje požara postaje vrlo efikasno, smanjujući štetu na imovini i povećavajući sigurnost ljudi unutar objekta. Automatizirani sustavi za dojavu i gašenje požara se najčešće nazivaju stabilni sustavi za dojavu požara a najčešće se koriste:

- Novec 1230
- Sustavi sa vodenom maglom
- CO2 sustavi
- Inergen
- Argonit
- Halotron
- FM 200
- Aerosolni sustavi
- Pjene za gašenje i namjenski sustavi za gašenje požara u cjevovodima, kuhinjama, el. ormari, server sobama
- Ansul sustavi



Slika 5.3. Block dijagram rada stabilnog sustava gašenja [24]

## **6. PRAVILNICI I ZAKONI**

Zakon o zaštiti na radu NN 71/14, 118/14, 154/14 , 94/18, 96/18

Zakon o zaštiti od požara NN 92/10

Zakon o privatnoj zaštiti NN 16/20

Zakon o provedbi Opće uredbe o zaštiti podataka NN 42/18

Pravilnik o izradi procjene opasnosti NN 112/2014

Pravilnik o izradi procjene rizika NN 112/2014

Pravilnik o sustavima za dojavu požara NN 56/1999

Pravilnik o sigurnosnim znakovima NN 91/2015

Pravilnik o hidrantskoj mreži za gašenje požara NN 8/2006

Pravilnik o provjeri ispravnosti stabilnih sustava zaštite od požara NN 44/12, 98/21, 89/22

Pravilnik o otpornosti na požar i drugim zahtjevima koje građevine moraju zadovoljiti u slučaju požara NN 29/2013

Pravilnik o zaštiti od požara u skladištima NN 93/2008

Pravilnik o zaštiti od požara u ugostiteljskih objekata NN 100/1999

Pravilnik o sustavima za dojavu požara NN 56/1999

Pravilnik o uvjetima i načinu provedbe tehničke zaštite NN, 198/03

Pravilnik o uporabi osobnih zaštitnih sredstava NN 5/2021

Pravilnik o uvjetima za osposobljavanje radnika za rad na siguran način NN 142/2021

Pravilnik o najmanjim zahtjevima sigurnosti i zaštite zdravlja radnika te tehničkom nadgledanju postrojenja, opreme, instalacija i uređaja u prostorima ugroženim eksplozivnom atmosferom NN 39/06, 106/07

Pravilnik o ovlaštenjima za poslove zaštite na radu NN 58/2022

## 7. ZAKLJUČAK

Integracija tehničkih sustava sigurnosti i zaštite predstavlja ključni element u stvaranju sveobuhvatnog sigurnosnog ekosustava koji učinkovito štiti ljude od ozljeda na radu, od nezgoda i imovinu. Kombinacija sustava tehničke zaštite omogućuje brzu identifikaciju, reakciju i prevenciju sigurnosnih prijetnji na različitim razinama. Primjeri kako iz teorije tako i iz prakse potvrđuju da integracija ovih sustava rezultira boljom sviješću o sigurnosti a operativno smanjenjem vremena reakcije te povećanjem efikasnosti i koordinacije sigurnosnih aktivnosti. Kroz stalni razvoj tehnologije i unapređenje integracijskih mogućnosti, očekuje se daljnje poboljšanje sigurnosti u različitim sektorima, također ključan dio u ovom segmentu je obrazovanje odgovornih osoba koje se zadužene za sigurnost. Važno je naglasiti da integracija tehnoloških sustava nije dovoljna sama po sebi. Potrebno je kontinuirano ulagati u razvoj sigurnosti i procedura te provođenje redovitih revizija i testiranja sustava kako bi se osigurala maksimalna pouzdanost. U konačnici, integracija tehničkih sustava sigurnosti i zaštite predstavlja važan korak prema stvaranju sigurnijeg okruženja i ozračja što su ključni preduvjeti za produktivan rad na radnom mjestu.

## 8. LITERATURA

Knjige i stručni članci:

- [1] Sandro Šegedin, Damira Trut, Zakon o privatnoj zaštiti s obrazloženjem i metodologijom provedbe nadzora
- [2] Protuprovalni sustavi zaštite (CROSBİ ID 341332), Dokmanović, Goran Rijeka, Tehnički fakultet, 2005
- [3] Protuprovalna vrata: Zašto su dobra i na što obratiti pažnju kod kupovine, <https://baustela.hr/app/uploads/2023/01/protuprovalna-vrata-2048x1365.jpg>, pristupljeno 15.4.2024.,
- [4] Mediteran security <https://www.mediteran-security.hr/portfolio.html>, pristupljeno 15.4.2024.,
- [5] Microcosm, <https://www.microcosm.com/images/what-is-software-protection-blogpost-banner.jpg>, pristupljeno 18.4.2024.,
- [6] Obrazac projektni zadatak, [https://www.academia.edu/39383038/Prilog\\_1\\_Obrazac\\_za\\_projektni\\_zadatak](https://www.academia.edu/39383038/Prilog_1_Obrazac_za_projektni_zadatak), pristupljeno 19.4.2024.,
- [7] Sustavi kontrole pristupa i video nadzora Kamir, <https://kamir.hr/sustavi-kontrole-pristupa>, pristupljeno 19.04.2024., <https://kamir.hr/sustavi-videonadzora>, pristupljeno 19.04.2024.,
- [8] Time & attendance controllers, <https://jantar.si/en/products/time-and-attendance-controllers/>, pristupljeno 29.4.2024.,
- [9] Sustavi IP portafonije, <https://kamir.hr/sustavi-ip-portafonije>, pristupljeno 29.04.2024.,
- [10] Software prime WebTime - primion Technology AG priručnik
- [11] Parkilo smart solutions, <https://parklio.com/en/parking-solutions/anpr>, pristupljeno 02.05.2024.,
- [12] CCTV: From Light to Pixels: Damjanovski, Vlado, 2013.,
- [13] AM Computers, <https://amcomputers.ba>, pristupljeno 02.05.2024.,
- [14] VBS Power Sustavi, <https://vbs-power.hr>, pristupljeno 07.05.2024.,
- [15] Zbirka propisa o zaštiti od požara i vatrogastvu, Jukić, Kirinčić, 1995.,

- [16] Priručnik za osposobljavanje vatrogasnih dočasnika i časnika, Željko Popović 2006
- [17] Centar za zaštitu na radu, <https://centarznr.hr/en/plan-evakuacije-i-spasavanja-kako-ga-izraditi/>, pristupljeno 07.05.2024.,
- [18] Tehnoservis, <https://www.tehnoservis.net>, pristupljeno 11.05.2024.,
- [19] Pravilnik o hidrantskoj mreži za gašenje požara NN 8/2006
- [20] Vatrozaštita, <https://vatrozastita.com/wp-content/uploads/2021/01/zidni-hidrant.jpg>, pristupljeno 07.05.2024.,
- [21] East Orange, NJ <https://www.eastorange-nj.gov/ImageRepository/Document?documentID=984>, pristupljeno 11.05.2024.,
- [22] Zaštita EU, <https://zastita.eu/zastita-od-pozara/stabilni-sustavi-za-gasenje-pozara/>,
- [23] Sigurnosni aspekti poslovanja benzinskih postaja INA d.d. (CROSBI ID 235159) Dundović, Pavliček, Hodak, 2011
- [24] Researchgate prikaz, <https://www.researchgate.net/profile/Amgad-Muneer-2/publication/345062499/figure/fig2/AS:952624572538880@1604134805853/Flowchart-of-the-Proposed-System-23-Placements-of-the-sensors-Real-life-application.ppm>, pristupljeno 15.05.2024.,
- [25] Directa radno vrijeme, <https://www.directa.hr/images/proizvodi/oc500m.png>, pristupljeno 27.05.2024.,
- [26] Global Security CDS, <https://www.global-security.hr>, pristupljeno 27.05.2024.
- [27] Prilog 3. Tehnička dokumentacija sa grafičkim priložima <https://www.hac.hr/files/shares/2018-04/Prilog%203.%20Tehni%C4%8Dka%20dokumentacija%20sa%20grafi%C4%8Dkim%20priložima.pdf>, pristupljeno 27.05.2024.

## 9. PRILOZI

### 9.1. Popis slika

Slika 3.1. Protuprovalna vrata	3
Slika 3.2. CDS-Centralni dojavni sustav	4
Slika 3.3. Simbolika softverske zaštite	5
Slika 3.4. Primjer izgleda projektnog zadatka	9
Slika 3.5. Zapisnik o obavljenom tehničkom prijemu	11
Slika 4.1. Kontroler sustava kontrole pristupa	13
Slika 4.2. RFID čitač s tipkovnicom	14
Slika 4.3. Primjer elektromagnetske (lijevo) i električne (desno) brave	14
Slika 4.4. Grafički prikaz procesa kontrole pristupa	15
Slika 4.5. Čitač otiska prstiju pri sustavu kontrole pristupa	16
Slika 4.6. Primjer RFID terminala i terminala s čitačem otiska prsta	17
Slika 4.7. Napajanje za terminale	18
Slika 4.8. Jantar Codeks TA aplikacija za radno vrijeme	19
Slika 4.9. Grafički prikaz procesa sustava evidencije radnog vremena	19
Slika 4.10. Primjer vanjske jedinice s jednom tipkom i s tipkovnicom	21
Slika 4.11. Primjer unutarnje jedinice sustava digitalne portafonije	22
Slika 4.12. Način rada sustava digitalne portafonije	22
Slika 4.13. Očitavanje registarskih oznaka	23
Slika 4.14. Parklio ANPR parking sustav	25
Slika 4.15. Grafički prikaz digitalnog sustava videonadzora	27
Slika 4.16. Grafički prikaz analognog sustava videonadzora	28
Slika 4.17. Box kamera	28
Slika 4.18. Bullet kamera	29
Slika 4.19. Dome kamera	29
Slika 4.20. PTZ kamera	29
Slika 4.21. Analogni (lijevo) i digitalni (desno) snimač	30
Slika 4.22. Softver za sustav videonadzora	30
Slika 4.23. Alarmni protuprovalni sustav	32
Slika 4.24. Evakuacijski plan	35
Slika 4.25. Evakuacijski terminal	36



Slika 4.26. Zidni hidrantski ormar	37
Slika 4.27. Sustav vanjske hidrantske mreže	39
Slika 5.1. Block dijagram integracija tehničkih sustava sigurnosti	43
Slika 5.2. Kontrola pristupa i evidencije radnog vremena	44
Slika 5.3. Block dijagram rada stabilnog sustava gašenja	48

## **9.2. Popis tablica**

Tablica 4.1. Podjela stabilnih sustava za gašenje požara [27]	40
---	----