HRVATSKI OGRANAK
MEĐUNARODNOG VIJEĆA ZA VELIKE
ELEKTROENERGETSKE SUSTAVE – CIGRE

10. simpozij: Povijest i filozofija tehnike
Zagreb, 23. – 25. studenoga 2021.

Franjo Jović
FERIT Osijek
fjovic90@gmail.com

Borislav Balać
R Jet-Robotics, Zagreb
boris.balac@r-jet-robotics.hr

00-00

ENTROPIJSKI MODELI SIGURNOSTI

Sažetak: Entropija je povijesni inženjerski alat izučavanja svrsishodnih mehanizama, a ponajviše strojeva s unutrašnjim izgaranjem (otac i sin Carnot, 1803). Pojavom Carnapa (1956) entropija postaje alat upotrebljiv pri istraživanju svrsishodnosti struktura i informacije u prostoru i vremenu. Prikazana je razrada Carnapove entropije na jednostavne sigurnosne situacije. Dana je osnovna informacijsko-sigurnosna mjera. Složenije sigurnosne situacije poput pandemije zahtijevaju holistički pristup sigurnosnim postupcima gdje se mora uključiti impersonalnost kontrole štićenog prostora. Dan je primjer jednog takvog rješenja.

Ključne riječi: entropijska mjera, štićeni prostor, neosobni nadzor, pandemija

Uvod

Postoji više definicija pojma sigurnosti. Sam pridjev 'siguran' označava (Collins): 1. Nepostojanje opasnosti, štete… 2. Oslobođenje od straha, brige …, 3. U sigurnom posjedu, 4. U stanju kada neće promašiti, olabaviti se, izgubiti se… 5. Oslonjiv, izvjestan . Prema

Fischeru i Greenu „sigurnost podrazumijeva stabilni i relativno predvidiv okoliš u kojem neki pojedinac ili grupa može izvršavati svoje postupke i operacije bez štete ili straha od smetnji ili ugroza“ [1]. Uobičajena definicija sigurnosti može biti: plaćena usluga u zaštiti ljudi, informacije ili vrijednosti za osobno ili zajedničko dobro, Craighead [2]. Osobna ili komercijalna sigurnost se može smatrati kao dobava plaćenih usluga kojima se sprečava neželjeno, nedozvoljeno ili štetno postupanje s organizacijskim dobrima, Post i Kingsbury [3].

U proširenju na državnu sigurnost ovo se miješa i grana u dva smjera: vojna i policijska sigurnost, Brooks [4], gdje je s jedne strane korištenje resursa za obranu ljudi od vanjske agresije a s druge strana korištenje resursa za kontrolu vlastitih građana. Neki autori pod sigurnosti smatraju prevenciju kriminalnih radnji, tehnologiju sigurnosti, upravljanje rizikom ili prevenciju gubitaka, Coole i Brooks [5]. Sigurnost može biti sve od navedenog čime se samo zamagljuje pojedinačno određeni interes cilja sigurnosti. Sigurnost može predstavljati jako različito značenje za razne ljude, s obzirom na vrijeme, mjesto i kontekst situacije ili procesa, Davidson [6]. Američko društvo za industrijsku sigurnost (ASIS) je ustanovila da svaki puta kada mislimo da smo postavili definiciju sigurnosti, ista nam izmakne.

Sigurnost (engl. security) se po učestalosti najviše pojavljuje kao sinonim s pojmom zaštite a po sličnosti s pojmom stabilnosti. Ne treba je brkati s pojmom procesne sigurnosti (engl. safety) koja se primarno odnosi na osobnu ugroženost u rizičnim situacijama, dakle na neugroženost, bezbjednost, stanje tehničke opreme i prometa u procesnoj namjeni, službi prometa, kretanja po vanjskom prostoru ili u sličnim rizičnim situacijama. Dakle sigurnost (security) se odnosi na *zaštićenost organizacije* od vanjske i unutrašnje ugroze a osobna bezbjednost (safety) na *smanjenje izloženosti riziku pojedinca* pri izvršavanju svojih zadataka.

Strukturalno je sigurnost povezana s dva vida entropije: termodinamičkom i Carnapovom entropijom. Termodinamička entropija razmatra vremensku degradaciju nekog objekta uređaja ili procesa. Carnapova entropija razmatra *aranžmana okolnosti uporabe danog sklopa, uređaja ili sustava tako da se prilagođuje danoj svrsi* [7], u ovom slučaju sigurnosti.

1. Pad razine sigurnosti

Pad razine sigurnosti definira se kao degradacija mikroskopskih sastavnica preko cijelog sigurnosnog sustava kao rezultat promjene znanja, kulture ili ekonomskih čimbenika, Coole i Brooks [5]. Upravljanje sigurnošću trebalo bi primarno biti usmjereno na upravljanje entopijskim procesima koji degradiraju projektiranu razinu sigurnosti sustava. Kada se dogodi degradacija ona slijedi učinak kretanje odozdola prema gore (bottom-up). Entropijskim učincima može se dati mjera kako bi se ona mogla primijeniti na projektiranje, primjenu i vođenje održavanja učinkovitog sustava sigurnosti organizacije.

Osnovno svakom mjerenju sigurnosnog sustava jest postojanje modela ponašanja njegovog probijanja.

Protumjere izvodive funkcijom zastrašivanja, detektiranja, kašnjenja, odgovora i oporavka su onda praktične mjere koje se poduzimaju u sustavu zaštite a prema modelu probijanja [1,5]. Da bi sustav zadržao svoju učinkovitost ove funkcije je najbolje primjenjivati slijedno. Ove funkcije su međutim izložene degradaciji koja vodi do grešaka u sigurnosnom odzivu. Zbog inherentne dijalektičnosti da veći stupanj sigurnosti dovodi do njezine veće samozaključanosti potrebno je razmotriti i holonski pristup.

1.1. Holonski model sigurnosnog sustava

Potpuno drugačiji pristup degradacije sigurnosti postoji u holonskom modelu svijeta Kena Wilbera [8]. U koncepciji svijeta po Kenu Wilberu holon je osnovna gradbena jedinica hijerarhije. U hijerarhije međutim vladaju odnosi koje možemo sa stajališta sigurnosti najkorisnije opisati kao empatičnima: niži sloj se podvrgava apsolutno pod ingerenciju višeg sloja a viši sloj posjeduje neograničenu pozitivnu emociju – ljubav – prema nižem sloju. Ovakav svijet beskompromisno postoji na atomsko- molekularnoj razini dok se izmiče na višim razinama hijerarhije holona, da bi naoko potpuno izblijedio u sigurnosnim sustavima, koja barataju pojmom ugroženost ili straha kao njegovom psihološki manifestnom iskazu, kao antipodu empatije.

Dakle po Wilberu bi snižavanje sigurnosti nastalo iz pada empatije u sustavu. Svjedoci smo namjernom ili manipuliranom porastu straha i padu empatije u društvu te tim prije porastu sigurnosnih ugroza.

2. Entropijski model – osnovni tipovi i primjene

Entropijski model svijeta dosta je konfuzan i naoko proturječan, jer izgleda da postoji onoliko entropija koliko postoji procesa. Tu situaciju možda najbolje opisuje jedna rečenica von Neumanna (cit.): „Nitko ne zna što je zapravo entropija“ [9]. Četiri su glavna pitanja koja se postavljaju pred entropijom. 1. Koliko entropija postoji? 2. Koje je fizikalno značenje entropije. 3. Je li entropija subjektivna ili objektivna veličina. 4. Je li entropija na bilo koji način povezana s informacijom [7]. Entropijski model sigurnosti primjenjiv je na degradacijske procese i opisan je u radu Coolea i Brooksa [5].

Bez obzira na koji pojam entropije se pozivamo, radimo ili sa skupovnim, masovnim pojavama, kao kod termodinamičke entropije ili s pojedinačnim situacijama kao kod Carnapove entropije [7].

2.1. Razrada modela rizičnosti po Carnapu

Ciljna ili teleonomska entropija razmatra entropiju pojedinačnih objekata u nekoj ciljnoj strukturi. Npr. entropiju rasporeda stolaca u učionici u svrhu uočavanja postignutog "reda u učionici". Mjera podjele prostora u tom slučaju određuje prostorne segmente Voronojeva dijagrama koje "zauzimaju" pojedini predmeti[1]. Odnos veličina tih prostora i njihova razdioba prema traženoj ciljnoj raspodjeli „reda u učionici" određuju trenutno stanje ciljne entropije.

Teleonomsku entropiju je prvi izrazio filozof Rudolf Carnap (1956.). Ona obuhvaća izračun informacije u danom prostoru stanja prema informaciji željenog prostora stanja, i dinamiku tog kretanja [7].

Temeljno pravilo Carnapove entropije jest da entiteti ustroja pravično dijele svoj fazni prostor. Entiteti su obično pretpostavljeni kao točkasti elementi, zvani mjerne točke. U konačnici logaritam udjela prostora entiteta ustroja pomnožen s udjelom daje informacijski sadržaj udjela tog entiteta. Zbroj svih informacijskih sadržaja svih entiteta daje iznos entropije danog ustroja u danom faznom prostoru. No mjera je uvijek bit po jedinici volumena faznog prostora, npr *bit/m*^{3}.

Rudolf Carnap (1956) uveo je opći, *n*-dimenzijski, prostor sustava koristeći sustavski prostor od *n* varijabli unutar teorijskih granica od R^{μ}, μ je u maksimumu jednak *n*. Svaka sustavska varijabla u_i, u gornjem slučaju prostorne varijable *X* i *Y* dana je unutar svojih minimalnih i maksimalnih granica vlastitog prostora ϕ_i. Tako svaki dvo, tro ili više – dimenzijski prostor proizvodi pripadni Voronojev dijagram. Odgovarajući prostor e_j koji određuje neka ćelija u tom prostoru dan je za svaku mjernu točku $b_j(u_{i1}, u_{i2})$ kriterijem najmanjeg razmaka prema susjednim ćelijskim mjernim točkama.

Povezivanja relativnog omjera svakog zauzetog prostora i teorijske granice mogućnosti prostiranja istog, dvojni logaritam te relacije naziva se Carnapova entropija[2] [7,10]

$$I_C = -\sum_j \frac{e_j}{R^{\mu}} ld \frac{e_j}{R^{\mu}} \text{ (bit/volumen prostora stanja)} \qquad (1).$$

[1]Georgij Voronoj (1868–1908), ruski i ukrajinski matematičar

[2] Dok se Voronojev dijagram odnosi na općenitu pravilnost zauzimanja prostora za Carnapovu entropiju to mora biti minimalni prostor rasprostiranja kinematičkih točaka tijela, odnosno ćelija, relevantnih za dani opis aranžmana okolnosti.

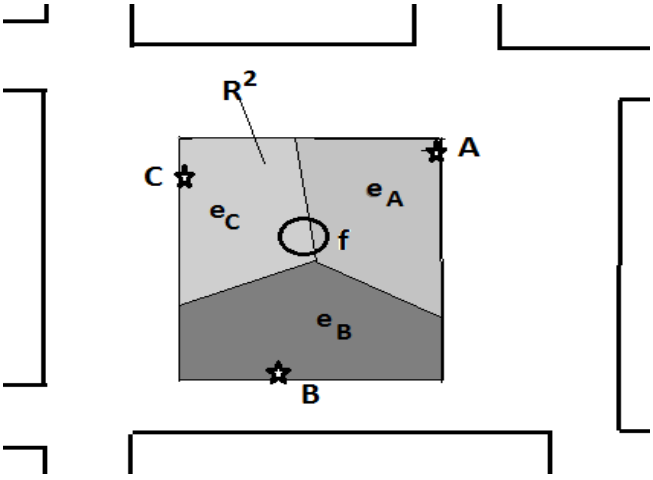
Carnapova entropija ne daje neka objašnjenja za slučaj da elementarne mjerne točke nisu istog sadržaja, npr iste mase!

2.2. Carnapov jednostavni model sigurnosti

Carnapov jednostavni model sigurnosti ilustriran je slikama 1. i 2. [7]. Vremensko-prostorna trajektorija sustava proizvodi dinamički Voronojev dijagram koji se može obilježiti i usporediti sa željenom teleonomskom trajektorijom sustava. Odatle Carnapova entropija može mjeriti entropiju teleonomskih sustava. Znajući da su svi tehnički uređaji ciljne namjene onda je Carnapova entropijska mjera njihov prirodni informacijski alat.

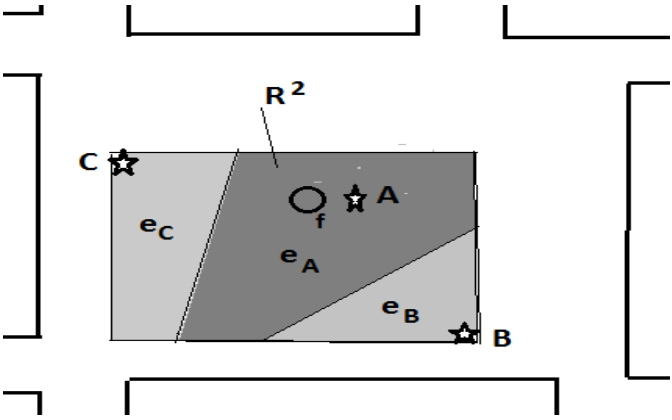
Razmotrimo jednostavan primjer, slika 1., gdje je nadzorna kamera na većem trgu u jednom trenutku identificirala tri potencijalno opasne osobe, A, B i C. Zanemarimo li ostale osobe i ogradimo li njihov maksimalni prostor, zvan fazni prostor R^2 koje one obuhvaćaju te ga 'pravično podijelimo' među njima dobili smo Voronojev dijagram Carnapove entropije u dvije dimenzije za te osobe. Iz relativnog udjela faznih podprostora su e_A, e_B i e_Cu faznom prostoru R^2 mogli bismo izračunati određenu mjeru rasporeda praćenih osoba, zvanu Carnapova entropija, no zaključiti o nečemu možemo tek kada bismo znali kakav je dogovor među praćenim osobama, to jest što im je cilj.

Slika 1. Prikazuje rizičnu situaciju prikazanu u radu [9].



Sl. 1. Voronojev dijagram Carnapove entropije za situaciju kada tri potencijalno opasne osobe A, B i C eventualno planiraju odložiti nešto u fontanu 'f' na trgu; pripadni prostor je R^2a podprostori su e_A, e_B i e_C dobiveni kriterijem najmanjeg razmaka prema susjednoj mjernoj točci (A, B ili C)

Slika 2. prikazuje ciljnu situaciju kada osoba A prilazi fontani. Razvidna je promjena u podjelama faznog prostora R^2 prema slici 1. Ona odražava i u kontinuiranoj promjeni entropije prikazane scene. No istu entropiju dobili bismo ako bi se zamijenile uloge osoba, što ukazuje na određene granice entropijskog opisa u smislu praćenja svrsishodnosti situacije. No ako bismo znali cilj akcije terorista entropija bi mogla biti egzaktno mjerilo izvršenja tog cilja čak i prije njegovog izvršenja. Dakle, slika 2. prikazuje promjenu te situacije.



Sl. 2. Ciljna situacija na trgu: osobe C i B su očigledno poslužile za odvlačenje pozornosti a osoba A je prišla fontani; vidljive su razlike u udjelima u faznom prostoru sada prema onima na slici 1.

2.3. Proširenje primjene Catnapove entropije na sigurnosni prostor

Dva su osnovna pitanja na koja Carnapov entropijski model ne daje odgovor u kontekstu ciljnosti danog aranžmana okolnosti. Što kada su čestice u gibanju iz formule (1) nejednake i kako odrediti njihovu nejednakost u primjeni na sigurnosnu situaciju? Više je mogućih ishoda, ako zanemarimo varijable brzine kretanja i orijentiramo se tako na Voronojev prostorni pristup, od kojih izdvajamo dva:
1. dodjela diskretnih razina djelovanja na sigurnost pojedinim 'česticama'
2. dodjela kontinuiranih razina djelovanja na sigurnost pojedinim česticama

Ovdje zanemarujemo sinergijski učinak dviju i više 'čestica' u sigurnosnoj procjeni.

Međutim kakvugod vrstu razine odabrali ovaj faktor težine pojedine razine utječe na izraz u formuli (1). Ona naprosto ne pristaje uz navedene pretpostavke. Probajmo preurediti stoga formulu (1) tako da izbacimo brzine i uvedemo težine uz svaku 'česticu'.
Preuređena formula sada glasi

$$l_{cS} = \sum_{i}^{N} \frac{e_i \cdot w_i}{R} l\, d \frac{e_i w_i}{R},\ {}^{bit}/_{R} \qquad (2),$$

gdje je w_i težinski koeficijent procjene ugroze svake 'čestice' a R je jednak

$$R = \sum_{1}^{N} e_i w_i \qquad (3).$$

Primjerice za slučaj sa slike 2. i uz pretpostavku da se prostori geometrijski dijele na čestice A, B i C kao $e_A = \frac{2}{5}$, $e_B = \frac{7}{20}$ i $e_c = \frac{1}{4}$ tada je Carnapova entropija jednaka $I_C = -\left(\frac{2}{5} ld \frac{2}{5} + \frac{7}{20} ld \frac{7}{20} + \frac{1}{4} ld \frac{1}{4}\right) = -(-0{,}5288 - 0{,}5301 - 0{,}4999) = 1{,}5588\ {}^{bit}/_{m^2}$, a ako se pretpostave težine ugroza za česticu A kao 3, za česticu B kao 2 a za česticu C kao 1 onda je izraz za sigurnosnu Carnapovu entropiju u trenutku promatranja sa slike 2. a prema formuli (2) jednak

$$I_{CS} = -\left(\frac{24}{43} ld \frac{24}{43} + \frac{14}{43} ld \frac{14}{43} + \frac{5}{43} ld \frac{5}{43}\right) = -(-0{,}4135 - 0{,}5272 - 0{,}3611) = 1{,}3018\ {}^{bit}/_{Sm^2},$$

gdje je oznaka mjerne jedinice S mjera procjene ugroze po prostornom metru površine.

Za slučaj podjednakih podjela Carnapova prostora kao sa slike 1. $I_C = -3\left(\frac{1}{3} ld \frac{1}{3}\right) = 2{,}059\ {}^{bit}/_{m^2}$, a ako je težina ugroza za A jednaka 3, za B jednaka 2 te za C jednaka 1 onda je sigurnosna Carnapova entropija jednaka

$$I_{CS} = -\left(\frac{1}{6} ld \frac{1}{6} + \frac{1}{3} ld \frac{1}{3} + \frac{1}{2} ld \frac{1}{2}\right) = 1{,}7397\ {}^{bit}/_{Sm^2}$$

2.4. Brzina promjene sigurnosne situacije

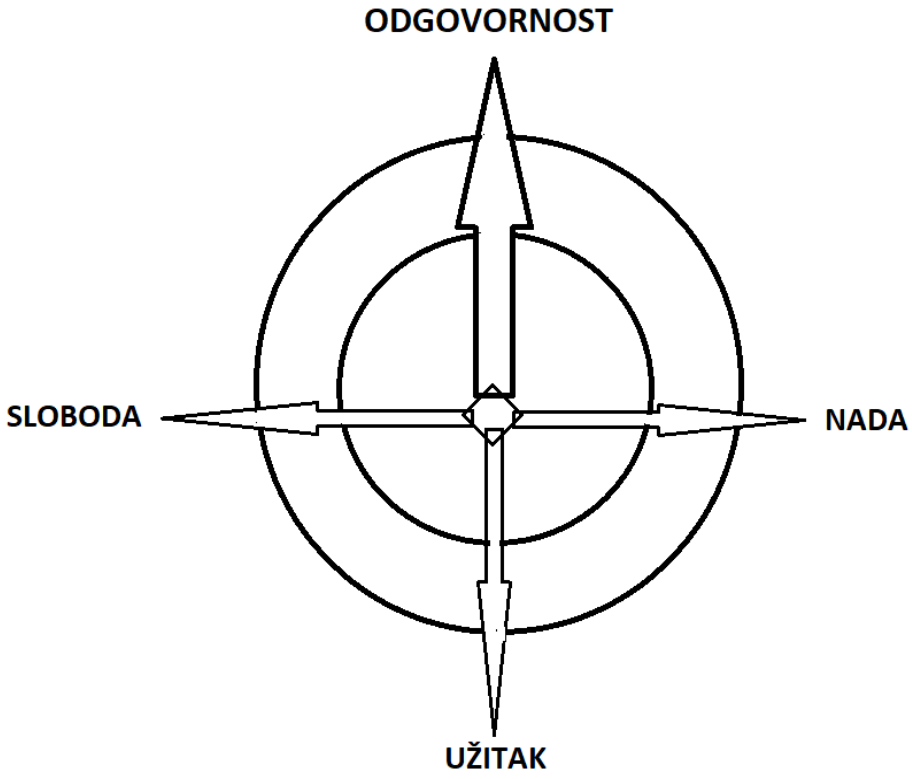
Brzina promjene sigurnosne situacije je složena mjera jer ovisi o brzini kretanja sigurnosnih agenata na sceni, njihovih međusobnih odnosa i promjena motiva s promjenom situacije. Tu odlučujuću ulogu igra faktor iznenađenja, kojim mogu biti podjednako pogođene i „obrambena“ i „napadačka pozicija“. Uz pretpostavku da je motivacijska komponenta postojana i da ulogu igra „raspored agenata“ u „ciljnoj formaciji“ onda je mjera procjene rizika jednaka mjeri postizanja „ciljne formacije“, odnosno Carnapova mjera odstupanja od te situacije. Zbog simetričnosti Carnapove mjere onda je najjednostavnije pratiti brzinu ispunjenja trajektorije agenata prema ciljnoj situaciji [10].

3. Složene sigurnosne ugroze

Pandemija predstavlja složenu sigurnosnu ugrozu jer svaki pojedinac predstavlja potencijalnog širitelja ugroze i istodobno žrtvu ugroze. Svijest o svojoj potencijalnoj opasnosti i istodobno ugrozi različito se manifestira kod pojedinaca i skupina. Pojedinac istodobno osjeća ograničenu slobodu npr kretanja ili druženja ali i odioznost prema potpunoj slobodi kretanja zbog mogućnosti zaraze. Ovu paradoksalnu situaciju opisuje više varijabli ljudskog ponašanja: sloboda, nada i tijek (užitak); u originalu: *freedom, hope and flow* [11]. Autor Csikszentmihalyi [12] argumentira da održavanje ljudske svijesti od atrofije zahtijeva brigu vlasti i njihovih aktivnosti prema ljudima kojima bi trebale spriječiti njihove zajednice od patnje, propadanja i smrti. U ovoj paradoksalnoj situaciji autor Kabigting [11] predlaže odgovornost kao četvrto stanje ljudske svijesti koja se operacionalizira u svjetlu teorija paradoksa koja omogućuje procvat ljudskosti i društva.

Odgovornost (engl. responsibility) ili osjećaj odgovornosti poziva se na obvezu zadovoljavajućeg obavljanja zadatka na osobnoj, organizacijskoj ili upravljačkoj razini izvedbe (11). Odgovornost se razlikuje od pojma ugovorne odgovornosti (engl. liability, accountability) koja je obvezna strana ponašanja neke stranke ili tvrtke. Odnosno, osoba preuzima odgovornost no nije utuživa zbog njezine provedbe. Opseg odgovornosti primarno pokriva pridružene ili operativne zadatke a ne preuzima moralne, etičke ili legalne vidove odgovornosti. Omogućavanje odgovornosti postaje ujedinjujući uvjet unutar slobode, nade i užitka [11].

Ovaj paradoks, koji prikazuje slika 3., navodi na definiciju paradoksa po Smithu i Lewisu [13], gdje su paradoks iskazi ili elementi koji su očigledno kontradiktorni po svojoj prirodi ili značenju ali koegzistiraju simultano i održavaju se u svom postojanju i prirodi te u ishodima osobnih i organizacijskih razlika. Ove razlike neizbježno rezultiraju u paradoksalnim tenzijama koje se mogu promatrati kao dileme ili suprotnosti, kao kompromisi i dijalektički parovi, ili se ispoljavaju kao paradoks koji utječe na način izbora ciljeva kojim se pojedinac izbavljuje od tenzije.



Sl. 3. Paradoks cjeline slobode, užitka i nade u ravnoteži s odgovornosti

Složene sigurnosne ugroze su svakako i pandemije jer se miješaju tehnički atributi sigurnosti (security) i procesne sigurnosti pojedine osobe (safety) da bi se na jednoj većem mjerilu postigao društveni cilj, obrana od pandemije.

4. Modeli uređaja za osiguranje prostora

Dva su osnovna modela uređaja za osiguranje prostora: nadzorno osobni i nadzorno impersonalni. Dok prvi podliježu zahtjevima iz GDPR standarda i EDPB smjernica drugi se mogu instalirati na svakom za vlasnika povoljnom mjestu. Oba uređaja moraju ustanoviti pridržava li se neka osoba unutar prostora štićenja zahtjeva koje je izdao vlasnik prostora. Na temelju te procjene moguće je stupanj ugroze numerički odrediti korištenjem izraza (2) i (3).

No zahtjevi za obradom podataka u navedenim uređajima se bitno razlikuju. Da bi utvrdili drži li se netko propisanih preporuka dovoljno je u prvom modelu

pamtiti njegovu sliku i naknadno ga prozivati na neposluh, dok je u drugom modelu indikacija neposluha anonimna i samo trenutno upotrebljiva.

Bez obzira na model, uređaj treba raspolagati s dovoljnom inteligencijom za izvršenje zadatka osiguranja prostora.

4.1. Izrada baze znanja i algoritam određivanja sukladnosti ponašanja sa zahtjevom sigurnosti

Koraci izrade baze znanja

Osnova baze podataka je 1000 visoko kvalitetnih sintetskih slika lica bez maske. Kako bi izgradili algoritam detekcije maske s visokom točnošću koristili smo tehniku augmentacije broja slika.

Na slici 4.a nalazi se nekoliko primjera slika iz baze znanja. Tehnika augmentacije slike koristi se kako bi se povećala baza podataka te tako dobio bolje prilagođeni algoritam za detekciju nošenja maske. Nad ulaznim slikama vršimo određene transformacije poput rotacije slike oko horizontalne osi, uvećanje i smanjivanje slike, nasumično izmjenjivanje svjetline slike kako bi dobili izmijenjene inačice ulazne slike. Za svaku sliku iz originalne baze znanja provodimo nasumične augmentacije odnosno izmjene te tako dobivamo još četiri različite izmijenjene slike, slika 4.b. Primjenom ove tehnike kao rezultat dobivamo bazu podataka koja sadrži 5000 slika te time osnovu za izradu boljeg i robusnijeg algoritma detekcije maske. Tehnika augmentacije slike koristi se i kao način za izbjegavanje prenaučenosti modela na slikama iz baze znanja. Prenaučenost modela predstavlja problem jer tada algoritam za detekciju maske vrlo loše generalizira te obavlja manje pouzdanu klasifikaciju na neviđenim slikama. Sprečavanjem prenapučenosti modela poboljšavamo točnost klasifikacije slika i robusnost samog algoritma.

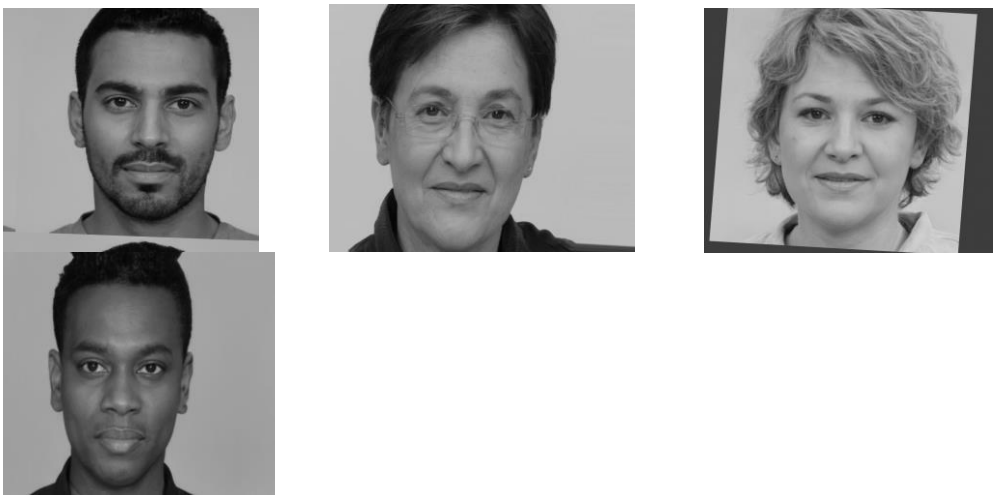
Sljedeći korak se primjenjuje kako bismo dobili dodatnih 5000 slika lica koje nose masku.

Proces se sastoji od prolaska kroz svaku od 5000 slika lica bez maske te detektiranja značajki lica. Detekcija značajki lica određuje gdje se na slici nalaze rubovi očiju, nosa, usta te crte rubova lica. To nam je potrebno kako bi na slike lica bez maske umetnuli sliku maske na odgovarajući dio lica. Navedeni program pronalazi značajke lica, određuje poziciju glave te aplicira sliku maske sa različitim uzorcima te različitim tipovima maske na dijelu lica gdje bi se inače nalazila maska. Rezultat programa nam daje 5000 slika lica koje sadrže masku na licu, slika 4.c.

Navedenom metodom dolazimo do dodatnih 5000 slika osoba koje nose maske. Inicijalna baza podataka od 1000 slika, sada sadrži 5000 slike osoba bez maske te 5000 slika osoba s maskom. Veličina baze podataka za izgradnju algoritma za detekciju maske daje nam dovoljno robustan model za primjenu u našoj aplikaciji.

Slika 4. Prikazuje dio korištene baze znanja za anonimno određivanje ispunjavanja temeljnog zahtjeva sigurnosti korištenja prostora – nošenja maske.

Sl. 4.a Početna baza slika za učenje



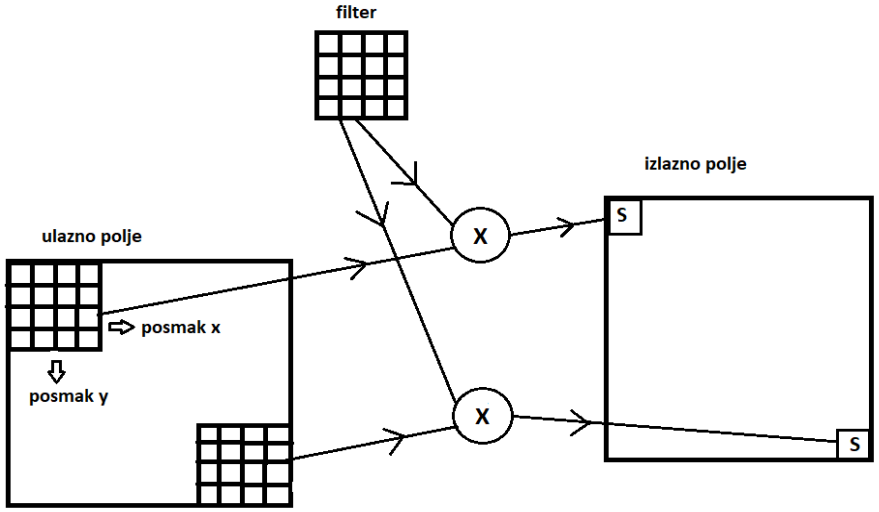
Sl. 4.b Augmentirana baza znanja za učenje

Sl. 4.c Početna baza znanja lica s atributom maske

Sl. 4. Tri osnovna koraka izgradnje baze znanja

Mehanizam učenja

Kao algoritam detekcije maske lica korištena je duboka neuronska konvolucijska mreža pod nazivom Xception [14]. Konvolucija je postupak opisan slikom 5. Glavni zadatak konvolucijskog sloja jest detektirati lokalne veze značajki s prethodnog sloja i preslikati iste na slijedeći sloj značajki. Kao rezultat konvolucija dobiva se receptivna polja značajki u dvodimenzijskom prostoru smanjene veličine. Tako polje značajki skladišti informaciju gdje se osobina pojavljuje na slici i koliko dobro odgovara na postavljeni filter. Odatle se svaki filter uvježbava prostorno s obzirom na položaj gdje se nalazi u volumenu na koji se primjenjuje. U kontekstu rada konvolucijske neuronske mreže konvolucija je linearna operacija koja uključuje množenje skupa težine zvane filter s ulaznim 2D poljem. Filter je manji od ulaznog polja i neka vrsta množenja bez preljeva je primijenjena između dijela polja veličine filtera i filtera točka po točka. Rezultat tog jediničnog množenja točaka se zbraja i uvijek daje jednu vrijednost, skalar. Postupak se sustavno ponavlja odozgora nadolje i slijeva udesno po ulaznom polju. Koraci promjene kretanja se mogu mijenjati. Kada filter sadrži traženi detalj slike tada se taj detalj savršeno poklapa s dijelom slike gdje se on nalazi i skalarna vrijednost to posebno ističe. Ovime se ističe postojanje neke osobine a manje mjesto gdje se ta osobina nalazi.



Sl. 5. Postupak konvolucije kojom se značajke određene filterom preslikavaju s ulaznog polja na suženo izlazno polje traženih osobina

Duboke neuronske mreže su naziv za slojne operatore koji sadrže osim ulaznog i izlaznog sloja i dva ili više skrivena sloja. One omogućuju modeliranje vrlo kompleksnih nelinearnih zavisnosti kakve pronalazimo u podacima. Duboke mreže koje sadrže konvolucijske slojeve nazivaju se konvolucijske neuronske mreže i najviše se koriste u primjenama računalnog vida. Konvolucijske neuronske mreže osim strukturne informacije imaju za cilj iskoristiti i dvodimenzijsku informaciju iz piksela slike što uvelike doprinosi točnosti obavljanja zadatka prepoznavanja.

Kako bi Xception model s visokom točnosnu klasificirao slike lica sa i bez maski potrebno je označiti sve slike iz baze znanja u koju skupinu pripadaju. Xception arhitektura je konvolucijska neuronska mreža koja se u potpunosti temelji na dubinski odvojivoj konvoluciji sa preskočnim vezama. Varijanta dubinski odvojive konvolucije korištena u ovoj arhitekturi prvo obavlja 1x1 konvoluciju, zatim prostornu konvoluciju po kanalima slike (RGB). Između ta dva koraka ne koristi se aktivacijska funkcija. Nakon svakog konvolucijskog sloja, kao i sloja dubinski odvojive konvolucije, slijedi sloj normalizacije nad grupom skalara. Normalizacija nad grupom doprinosi da mreže lakše uče na podatcima koji su normalizirani, a to znači preslikani u podatke čija su srednja vrijednost ništica i imaju jediničnu varijancu. Osim pomoći u treniranju, normalizacija vrši regularizaciju dubokog modela te omogućuje korištenje veće stope učenja. Regularizacija sprječava prenaučenost modela te tako model bolje generalizira za nepoznate primjere.

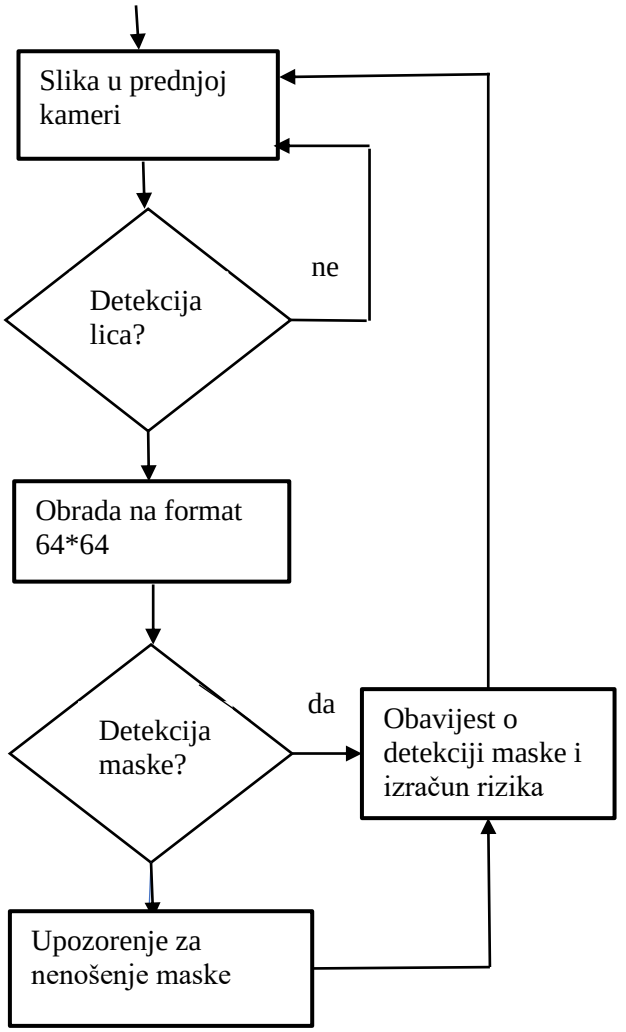
Učenje se obavlja koristeći bazu znanja na način da za učenje mreže koristimo 70% slika iz baze znanja, 20% slika kao validacijski set slika. Dio od 10%

slika mreža nije koristila za učenje nego za izračun točnosti klasifikacije. Učenje se obavlja dok se ne dosegne kriterij od 40 epoha. Jedna epoha predstavlja jedan prolazak svih slika za učenje kroz mrežu. Dakle učenje se završava nakon što sve slike za učenje izvrše izračun kroz model 40 puta. Nakon obavljenog učenja, naučena mreža se koristi za klasificiranje testnih slika. Na testnom skupu slika označeno je koje slike sadrže masku, a kojene, te tako možemo usporediti s izlazom mreže i izračunati točnost mreže na slikama koje mreža nije vidjela tijekom učenja. Navednim izračunom dolazimo do točnosti mreže od 93% odnosno do pogreška prepoznavanja maske od 7%.

Mehanizam prepoznavanja nošenja maske

Nakon izgradnje baze znanja i primjene postupka učenja pristupa se provjeri ispunjavanja kriterija zadovoljenosti ispunjenja osnovnog zahtjeva, nošenja maske,

slika 6.

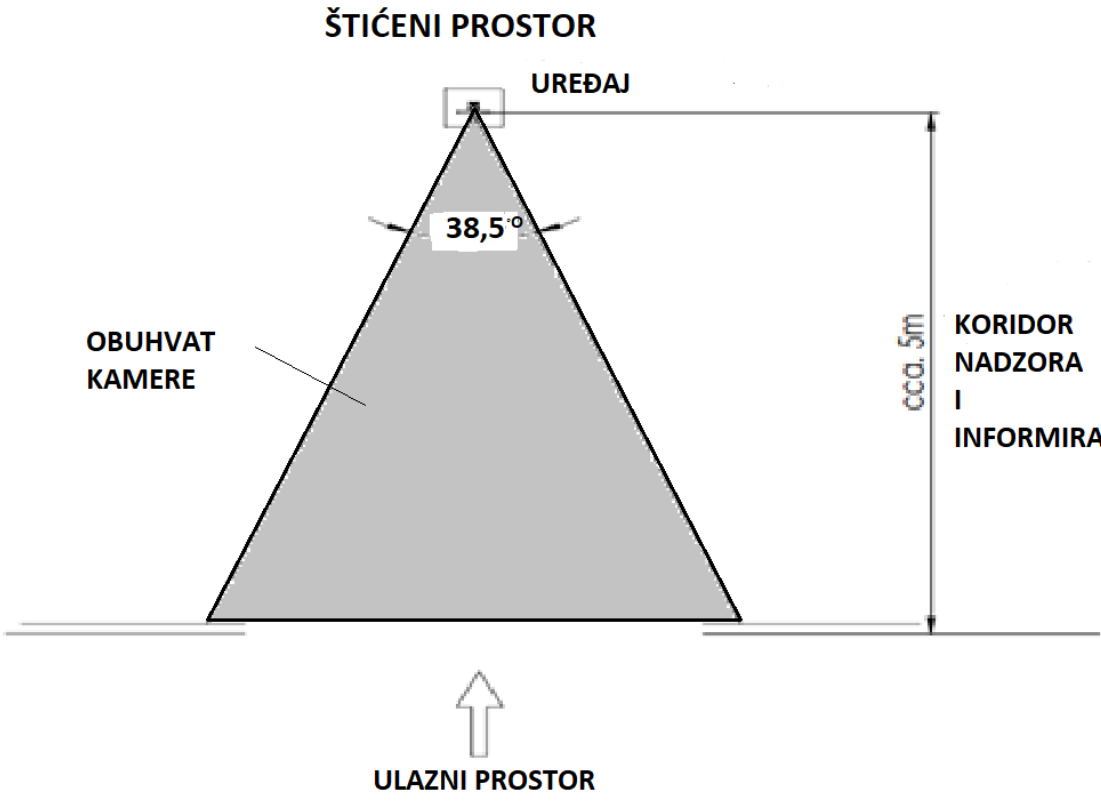


Sl. 6. Detaljniji dijagram toka kontrole nošenja maske

Pretprocesirana slika lica dimenzija 64x64 koristi se kao ulaz u algoritam za detekciju maske koji daje odluku da li osoba nosi masku. Ovisno o načinu rada aplikacije izdaju se informativne poruke ili poruke upozorenja. Cijeli proces analize slike se obavlja unutar < 0.3 sekunde te se provodi na svaku dostupnu sliku iz prednje kamere. Sustav ima očekivano visoku točnost na udaljenosti do 6 metara od postavljenog tablet uređaja u konvencionalno osvjetljenom štićenom prostoru.

4.2 Postav u štićeni prostor

Primjer postava uređaja u nadzirani prostor dan je slikom 7. za slučaj štićenja ulaza u objekt. Na ovaj način prostor postaje 'teritorijalno inteligentan' [15].



Sl. 7. Postav uređaja u koridor nadzora i informiranja

Rasprava i zaključak

Ne postoji jedinstven entropijski pristup sigurnosnim procesima. Pristup preko termodinamičke entropije može biti pogodan za korištenje pri popuštanju sigurnosnih mjera s duljim protijekom vremena poput skrivenih kvarova u mehaničkim dijelovima sigurnosnog sustava ili nestanka sigurnosnih podataka na medijima

nositeljima informacije. Drugi pristup zasnovan na Shannonovoj kodnoj entropiji, osim u teoriji kodiranja procesa, nema zdravo zasnovanu osnovicu jer je informacijsko-semantički potpuno indiferentan na promatrani proces. Treći pristup putem Carnapove entropije može obuhvatiti jednostavnije prostorno-sigurnosno okolnosti. Praćenje dinamike sigurnosne situacije može biti zamagljeno simetričnim izračunskim okvirom postupka, no svakako je nepristrano i dinamički dosta provedivo. Na prikazanom primjeru je uporabom algoritma za brzo raspoznavanje lica osigurana pravodobna reakcija uređaja od 0,6 s do 1,3 s, te depersonalizirano i prijateljsko ophođenje s korisnicima prostora na udaljenosti između 6 i 2 metra od uređaja.

Literatura

[1] R.J. Fischer, G. Green, (2004) *Introduction to Security*. Boston, MA: Butterworth-Heinemann.

[2] G. Craighead, (2003) *High-Rise Security and Fire Life Safety*. Woburn, MA: Butterworth-Heinemann.

[3] R.S. Post, A.A. Kingsbury,(1991) *Security Administration: An Introduction to the Protection Services*. Boston, MA: Butterworth-Heinemann .

[4] D.J. Brooks, *What is security: Definition through knowledge categorization*, 2009 Palgrave Macmillan 0955–1622, Security Journal 1–15.

[5] M. Coole, D. J. Brooks, *Do security systems fail because of entropy?* Journal of Physical Security 7(2), 50---76 (2014).

[6] M.A. Davidson, (2005) *A matter of degrees* . *Security Management* 49 (12) : 72 – 99 .

[7] F. Jović, Ž. Kozlina, A. Jović, Informacija o svrsishodnim mehanizmima, 9. PIFT 2020.

[8] V. Borš , *Integralna teorija Kena Wilbera*, FF press, Zagreb, 2012.

[9] M. Popovic, *Researchers in Entropy Wonderland: A Review of the Entropy Concept*. https://arxiv.org/abs/1711.07326.

[10] A. Pudmetzky, *Teleonomic Entropy Measuring the Phase-Space of End-Directed System*, Appl. Math. Comput. 162 (2) (2005) 695–705.

[11] J. Kabigting, (2021). *Responsibility: Enabling Human Consciousness and Flourishing Using Paradox Theory*. *Academia Letters*, Article 368. https://doi.org/10.20935/AL368.

[12] M. Csikszentmihalyi, M. (2014). *The politics of consciousness*. In T. J. Hämäläinen & J.Michaelson (Eds.), *Well-being and beyond* (pp. 271-282). Cheltenham, UK: Edward Elgar Publishing.

[13] W. Smith, M. Lewis, (2011). *Toward a theory of paradox: A dynamic equilibrium of organizing*. Academy of Management Review, 36(2), 381-403.

[14] F. Chollet, *Xception: Deep Learning with Depthwise Separable Convolutions*, https://arxiv.org/abs/1610.02357.

[15] Ph. Dumas, J-Ph. Gardère, Y. Bertachini, *Contribution of socio-technical systems theory concepts to a framework of territorial intelligence*, Caenti Huelva Oct 2007.

SECURITY ENTROPY MODELS

Summary: Entropy is a historic engineering tool for studying purposeful mechnisms mostly in combustion machines, father and son Carnot around 1803. Carnap proposed the entropy concept in 1956 for studying purposeful structure and information in time and space. Information-security measure based on Carnap entropy is proposed. More complex security situations like pandemy measure enforcement demand a holistic approach to security procedures where the impersonality of the surveillance of the protected area is the issue. An example of such an approach is presented.

Key words: Entropy measure, protected area, impersonal surveillance, pandemy

Franjo Jović i Borislav Balać