UPRAVLJANJE RIZICIMA OD PRIRODNIH I DRUGIH NESREĆA NA ELEKTRODISTRIBUTIVNOJ MREŽI KAO DIJELU KRITIČNE INFRASTRUKTURE

Edin GARAPLIJA, Institut za upravljanje rizicima INZA Beograd, Srbija
Velimir STRUGAR, Elektroprivreda Crne Gore AD Nikšić, Crna Gora

KRATAK SADRŽAJ

Globalne klimatske promjene su u poslednjim desetljećima bitno uticale na sigurnost elektrodistributivne mreže kao dijela kritične infrastrukture, kako na nacionalnom tako i na međunarodnom nivou. Svjedoci smo učestalih prekida prenosa električne energije uslijed prirodnih, tehničko-tehnoloških i drugih nesreća, u koje ubrajamo poplave, požare, zemljotrese, klizišta, orkanske vjetrove, mrazeve. Također, sve su prisutnije i globalne prijetnje od terorizma i sabotaže koji mogu značajno uticati na živote i zdravlje stanovništva, lokalnu ekonomiju i životnu sredinu. Ovakvi uticaji mogu reprodukovati nemir, strah i paniku u zajednici te mogu uticati na njen društveno-politički život. Upotreba modernih tehnologija i 3D GIS modela integrisanog pristupa identifikaciji, analizi i vrednovanju rizika, omogućava nam maksimalni preventivni pristup, ali i jačanje kapaciteta spremnosti i odgovora. Perspektiva ovakvog inovativnog pristupa je u permanentnom jačanju specijalističkih upravljačkih i operativnih kadrova kao nosilaca razvoja integrisanog sistema zaštite i spasavanja, te upravljanja rizicima na kritičnoj infrastrukturi.

Ključne reči: rizik, kritična infrastruktura, integrisani sistem, inovativna tehnologija, 3D GIS modeliranje

SUMMURY

Global climate change in the last decades has an important impact on the security of power distribution networks as part of critical infrastructure, on nationally and internationally level. We are witnessing frequent interruptions of electricity transmission due to natural, technical-technological and other accidents involving floods, fires, earthquakes, lendslides, storms, frosts. Also, there are more and more global threats of terrorism and sabotage that can have a significant impact on the lives and health of the population, the local economy and the environment. Such impacts may reproduce discomfort, fear and panic in the community and may affect its social and political life. The use of modern technologies and 3D GIS models of integrated approach to identification, analysis and risk assessment, enable maximum preventive approach as well as capacity building of readiness and responsiveness. The perspectives of such an innovative approach are the permanent strengthening of specialist management and operational staff as the mainstay of the integrated protection and rescue system, and risk management on critical infrastructure.

Key words: risk, critical infrastructure, integrated system, innovative technology, 3D GIS modeling

Kontakt informacije o autorima – Times New Roman 8

UVOD

Svjedoci smo značajnih globalnih klimatskih promjena u prethodnim desetljećima koje su bitno uticale na život i rad savremenog društva. Također, ove promjene značajno utiču i na sigurnost elektrodistributivne mreže kao dijela kritične infrastrukture naročito sa aspekta da je savremeno društvo nezamislivo bez permanentne upotrebe električne energije. Učestali prekidi prenosa i distribucije električne energije uslijed prirodnih, tehničko-tehnoloških i drugih nesreća, u koje ubrajamo poplave, požare, zemljotrese, klizišta, orkanske vjetrove, mrazeve značajno utiču na sve sfere u savremenom društvu, ponekad i dramatično. Također, u ambijentu sve češćih globalnih prijetnji od terorizma i sabotaža koje mogu značajno uticati na živote i zdravlje stanovništva, lokalnu ekonomiju i životnu sredinu potrebno je iznalaziti brza i efikasna rješenja koja će se primijeniti kako preventivno

tako i korektivno. Ovo naročito zbog spoznaje da ovakvi uticaji nerijetko podstiču nemir, strah i paniku u zajednici te mogu uticati na njen društveno-politički život.
Uzimajući u obzir da se elektrodistributivna mreža zbog svog značaja za normalno funkcionisanje društva u cjelini, s pravom svrstava u najranjivije kategorije kritične infrastrukture, ne možemo zanemariti i uticaje prekida distribucije električne energije uslijed namjerne ili nenamjerne ljudske greške ili nemara. Također, opšte poznata činjenice je da u čitavom elektroenergetskom sistemu (EES) Srbije distributivna mreža odnosno njeni djelovi imaju najveću vjerovatnoću pojave prekida u radu. Na prvom mestu zbog svoje široke rasprostranjenosti i osetljivosti nadzemne mreže na vremenske prilike naročito u brdsko-planinskim predelima. Osim toga, pouzdanost rada elektrodistributivnog sistema je obrnuto proporcionalna starosti elemenata koja na mnogim mestima u sistemu iznosi i preko 40 godina. Otežan pristup pojedinim deonicama dugačkih nadzemnih vodova u brdsko-planinskim predelima, starost elemenata sistema u ovim predelima i izloženost oštrijim klimatskim uslovima doprinose smanjenoj pouzdanosti rada čitavog elektrodistributivnog sistema. Zbog toga je potrebno pronaći način za preventivno uočavanje i prevazilaženje ovih problema korišćenjem novih tehnologija i metoda koje se manje oslanjaju na ljudski faktor.
Savremene tehnologije i 3D GIS modeli integrisanog pristupa identifikaciji, analizi i vrednovanju rizika, nude ogromne mogućnosti naročito kada je u pitanju prevencija ali i jačanje kapaciteta u pogledu spremnosti i odgovora na alertnu situaciju. Ovaj inovativni pristup je posebno značajan kad je u pitanju upravljanje rizicima na kritičnoj infrastrukturi, a posebno u smislu permanentnog jačanja specijalističkih upravljačkih i operativnih kadrova kao nosilaca razvoja integrisanog sistema zaštite i spasavanja.

POJAM KRITIČNE INFRASTRUKTURE

Pojam kritične infrastrukture označava državnu imovinu, sistem ili njihov dio, neophodan za održavanje vitalnih društvenih funkcija. Funkcionisanje modernog društva, kako u redovnoj, tako i u vanrednoj situaciji, nije moguće zamisliti bez efikasne zaštite značajnih infrastrukturnih sistema i objekata te se kao jedan od primarnih i najznačajnijih sigurnosnih izazova novog doba nameće problem zaštite kritične infrastrukture. U kritičnu infrastrukturu ubrajamo: elektrodistributivne mreže, saobraćajne (kopno, more, vazduh) mreže, prehrambene mreže (hrana i voda), informacione i komunikacione mreže i drugu infrastrukturu neophodnu za normalno funkcionisanje društva u cjelini. Kritična infrastruktura je zbog svog značaja veoma važan segment državne, lokalne i opšte sigurnosti. Ljudi su postali svjesni da ne mogu da štite sve i uvijek te da moraju da kategoriziraju koja je infrastruktura od ključnog (presudnog) značaja za zajednicu. U posljednjih desetak godina, pitanje kritične infrastrukture je posebno postalo značajno. Moderni stil života i zavisnost ljudi i privrede od električne energije i interneta (komunikacije uopšte) je svakim danom sve veća i veća.[1] U zavisnosti od različitih kriterija, a u cilju definisanja kritične infrastrukture, postoji potreba za boljim sagledavanjem različitih tipova kritične infrastrukture. Sagledavajući značaj lokalne zajednice na društvo, ekonomiju i okolinu moguće je govoriti o kritičnoj infrastrukturi: na lokalnom, regionalnom (ekonomski ili kulturni región u državi), državnom i međunarodnom nivou. U zavisnosti od vremena potrebnog za zaštitom, kritična infrastruktura[2] može biti: stalna, privremena ili potencijalna. Stalna kritična infrastruktura je ključna infrastruktura za neke države, u principu je propisana zakonom ili nekim drugim strateškim dokumentom, a koja mora biti u fokusu sve vrijeme strateškog planiranja razvoja i održivosti društva. U kategoriju privremene kritične infrastrukture je moguće uvrstiti neke političke ili sportske događaje koji su kratki, ali koji su veoma važni za državu ili koji su međunarodno značajni. Za ove infrastrukture je poznato da će biti važne u neko buduće vrijeme ili tokom nekih događaja.
Potencijalna kritična infrastruktura je infrastruktura koja nije u fokusu, ali u nekim situacijama može biti veoma važna. Za tu infrastrukturu je poznato da može postati kritična infrastruktura u nekim prilikama, ali ove situacije se ne planiraju unaprijed. Sve vrste kritičnih infrastruktura se moraju uzeti u obzir kada se planira zaštita kritične infrastrukture. Veliki broj vrsta kritične infrastrukture znači da svi nivoi vlasti u državi ili u nekim organizacijama, na lokalnom, državnom ili međunarodnom nivou, treba da sinergijski učestvuju u zaštiti kritične infrastrukture, na način kako da iskoriste najoptimalnije sve svoje resurse. Iz tih razloga je neophodna uspostava integrisanog sistema za zaštitu kritične infrastrukture, u zavisnosti od nivoa vlasti i državne strukture. Zaštita

---

[1] Zemljotres na Haitiju, uragan Katrina u SAD-u, cunami u jugoistočnoj Aziji, cunami u Japanu, katastrofalne poplavei požari u Evropi, su također pokazali da prirodne katastrofe mogu imati razorne posljedice na infrastrukturu. Teroristički napad od 11. septembra 2001. godine u Sjedinjenim Američkim Državama, dao je novo značenje i novu dimenziju koncepta zaštite kritične infrastrukture. Teroristički napadi u Madridu, Londonu, Moskvi, Mumbaiju i Islamabadu su samo potvrdili potrebu za novim pristupom u zaštiti kritične infrastrukture.

[2] Kritična infrastruktura u odnosu na vlasništvo unutar jedne zajednice, može biti u posjedu: države, općine, privatnog lica, lica za upravljanje imovinom u državnom vlasništvu, u vlasništvu pravnih lica čiji su osnivači lokalne samouprave. S druge strane, to znači da može biti kritična infrastruktura u javnim, privatnim ili javno-privatnim rukama. Javno-privatno partnerstvo je od suštinskog značaja, jer se procenjuje da preko 85% od onoga što se može klasifikovati kao kritična infrastruktura u Sjedinjenim Američkim Državama je u vlasništvu privatnog sektora, dok je u Njemačkoj taj omjer privatizovane kritične infrastrukture preko 90%.

kritične infrastrukture je definisana kao strategija, politika i spremnost, da se zaštiti, spriječi, a kada je to potrebno i odgovori na napade na ove ključne infrastrukture i sredstva. Postoje različite definicije pojma Kritične infrastrukture, ali ćemo u ovom radu obraditi samo definiciju u skladu sa smjernicama Evropske Unije, kao strateškog geo-političkog opredjeljenja zemalja regiona, uključujući i Republiku Srbiju:
(a) „Kritična infrastruktura predstavlja imovinu, sistem ili njegov dio koji se nalazi na teritoriji zemlje članice (ili zemlje kandidata) i koji je neophodan za održavanje ključnih društvenih funkcija: zdravstva, bezbednosti, sigurnosti, ekonomskog ili socijalnog blagostanja, a čije bi ometanje ili uništenje imalo značajan uticaj na zemlju članicu“.[3]
(b) „Evropska kritična infrastruktura podrazumeva kritičnu infrastrukturu lociranu na teritoriji zemlje članice, čije bi ometanje ili uništenje imalo značajan uticaj na bar dve zemlje članice. Značaj poremećaja u funkcionisanju elemenata kritične infrastrukture treba da se proceni na osnovu kriterijuma međuzavisnosti. To podrazumeva efekte nastale kao rezultat međusektorske zavisnosti od drugih tipova infrastrukture“.
U okviru Evropske unije pod terminom kritične infrastrukture podrazumevaju se postrojenja, sistemi ili određene komponente tih sistema, koji su locirani u zemljama članicama i koji su esencijalni za obavljanje osnovnih funkcija država i Unije, zatim koji su neophodni za funkcionisanje zdravstva, za bezbednost članica i za ekonomsko i socijalno blagostanje građana, a čije bi otkazivanje ili ometanje funkcionisanja imalo znatan negativan uticaj na zemlje članice, a posredno i na čitavu Evropsku uniju.[4]
Kritična infrastruktura se sastoji od fizičkih i informacionih tehnoloških objekata, mreža, službi i materijalnih dobara, koji, ukoliko budu urušeni ili uništeni, mogu imati ozbiljan uticaj na zdravlje, bezbednost, sigurnost i ekonomsko blagostanje ili efikasno funkcionisanje vlasti. Ovu definiciju najčešće koriste institucije UN u obrazloženju sadržaja pojma - kritična infrastruktura.
Poučeni naučenim lekcijama, pojam zaštite kritične infrastrukture, moramo sagledavati i sa lokalnog nivoa. S tim u vezi može se izvesti definicija pojma lokalne kritične infrastrukture koja podrazumijeva sve sisteme i mreže čije bi se narušavanje i prekid odrazili na normalan život i funkcionisanje lokalne zajednice. Posebno mjesto definisanja kritične infrastrukture na lokalnom nivou zauzima elektrodistributivna mreža. Prisjetimo se izjave portparolke Rudarsko topioničarskog basena Bor, koju je dala početkom decembra 2014., za Radio Slobodna Evropa, da je Majdanpek u utorak u potpunom kolapsu:
“Bez električne energije Majdanpek ne liči na sebe. Nema struje, vode i grejanja. Ne funkcioniše mobilna telefonija, a slabo rade i fiksni telefoni. Ovakva situacija ne pamti se u poslednje tri decenije”.[5]

POJAM I KLASIFIKACIJA RIZIKA NA KRITIČNOJ INFRASTRUKTURI

Prema međunarodnom standadu za upravljanje rizicima i tehnikama procjenjivanja[6], rizici su kombinacija posledica nekog događaja (P) ili opasnosti i povezane vjerovatnoće njegovog nastanka. Posledice su negativni efekti katastrofe izraženi u pogledu ljudskih uticaja, ekonomskih i ekoloških uticaja, i političkih / društvenih uticaja.
U situacijama u kojima se vjerovatnoća pojave opasnosti određenog intenziteta može kvantifikovati, koristimo termin vjerovatnoća pojave. Kada je stepen uticaja nezavisan u odnosu na vjerovatnoću pojave opasnosti, što je često slučaj sa čisto prirodnim nepogodama, kao što zemljotresi ili oluja, rizik se može izraziti algebarski na sledeći način:[7]

Rizik = uticaj opasnosti (P) * vjerovatnoća pojave (V)

Jednostavan primjer: Rizik od oluje koja izaziva oštećenja (uticaj) od 10 miliona eura i za koju postoji vjerovatnoća da će se pojaviti u prosjeku jednom godišnje može se posmatrati kao isti rizik od oluje koja prouzrokuje štetu od 350 miliona eura, ali za koju nam je poznato iz prošlih iskustava da je vjerovatno da će se desiti samo jednom u 35 godina. Gdje veličina uticaja utiče na vjerovatnoću nastanka, tj. gdje ova dva kvantifikatora nisu nezavisna jedan od drugog, rizik ne može jednostavno biti izražen kao proizvod dva kvantifikatora, već mora da se izrazi kao funkcionalna veza. Isto tako, gdje uticaji zavise od spremnosti ili preventivnog ponašanja, npr. blagovremena evakuacija, postoje prednosti u izražavanju indikatora uticaja na više različitih načina. Posebno u analizi prirodnih opasnosti, uticaji su često izraženi u smislu ranjivosti i izloženosti. Ranjivost V je definisana kao karakteristike i okolnosti zajednice, sistema ili sredstva koje ga čine podložnim štetnim efektima opasnosti.

---

[3] Critical Infrastructure Protection in the Fightagainst Terrorism, Brussels, COM(2004)702, 2004.
4 Council Directive 2008/114/EC, On the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection, Official Journal of the European Union, L 345/75-L 345/82, 2008
5 SlobodnaEuropa.org
6 ISO 31010:2009
7 EU Smjernice za procjenu rizika, Smjernice Evropske Unije za procjenjivanje rizika SEC(2010) 1626 - od 2010. godine

Izlaganje E je sveukupnost ljudi, imovine, sistema ili drugih elemenata koji su prisutni u zonama opasnosti koje su na taj način predmet potencijalnih gubitaka.

$$\text{Rizik} = P*E*V \quad [8]$$

Upotreba koncepta ranjivosti čini jasnijom činjenicu da su uticaji opasnosti takođe i funkcija preventivnih i pripremnih mjera koje su upotrebljene za smanjenje rizika. Na primjer, za opasnost od toplotnog talasa može biti slučaj da mjere bihevioralne pripremljenosti, kao što su informacije i savjeti, mogu kritički smanjiti ugroženost populacije od rizika od prekomjernog broja smrtnih slučajeva. Djelotvorne mjere za prevenciju i spremnost na taj način smanjuju ranjivost, a samim tim i rizik. U zavisnosti od određenog analiziranog rizika, mjerenje rizika se može izvesti sa većim brojem različitih varijabli i izvršioca, u zavisnosti inter alia od složenosti lanca uticaja, broja uticaja koje su izvršioci razmatrali i potrebnog nivoa preciznosti. Generalno, složenost modelovanja i kvantifikacija faktora može se povećati sve dok navedeno isto tako poboljšava sigurnost. Stoga, kada kvantitativni modeli i dodatne varijable i faktori povećavaju kompleksnost bez istovremenog poboljšanja sigurnosti (u smislu pouzdanosti, prognoze i robusnosti), korišćenje više kvalitativnih procjena i stručnih mišljenja će u principu biti bolji izbor, i sa stanovišta efikasnosti resursa i nivoa transparentnosti.

Klasifikacija bezbjednosnih prijetnji i rizika po kritičnu infrastrukturu može se izvršiti na više načina. Tako, na primer, moguće ih je na osnovu porijekla podijeliti u tri izolovane kategorije:[9]

- Rizici od elementarnih nepogoda (prirodne nesreće)
- Rizici tehničke prirode, koji obuhvataju greške unutar sistema infrastrukture, koje se mogu dalje prema porijeklu uzroka podijeliti na:
    - one do kojih dovodi ljudski faktor: loše planiranje aktivnosti u okviru sektora, nesmotrenost operatera kritičnom infrastrukturom, neadekvatna kooperacija ili koordinacija aktivnosti i
    - one do kojih dolazi iz tehničko-tehnoloških razloga: otkazivanja mašina, greške na opremi ili greške u softveru koji se koristi u okviru nekog infastrukturnog sektora.
- Rizici iz grupe opšte bezbednosti, koji se dijele na:
    - fizičke (direktni teroristički napadi i sabotaže)
    - virtuelne (sajber-napadi).
    - ratni sukobi.

Rizici od elementarnih nepogoda mogu se posebno dijeliti na: hidrometeorološke rizike (poplava, cunami, požar, mraz, orkanski vjetar i sl.) i geološke (zemljotres, klizište, odron). Za sve vrste rizika od elementarnih nepogoda, zajednički sadržalac su anomalije u ponašanju prirode izazvane klimatskim promjenama i globalnim zagrijavanjem. Ovakvi rizici mogu biti i multi posljedični, odnosno jedan rizik može pokrenuti i drugi, dnosno druge. Npr. Ukoliko imamo obilne padavine koje mogu prouzrokovati bujične poplave, uobičajeno je da na terenu iste izazovu i odrone, odnosno klizanja tla, koja opet mogu dovesti do "prirodnog pregrađivanja" korita rijeka i iazivanju poplavnog talasa kakav se desio u Bosni (Topčić Polje) 2014.godine. Također, ove vrste rizika prate ogromne posljedice po živote i zdravlje ljudi, ekonomiju i društveno politička uređenja. Učestalost ove vrste rizika je u porastu, tako da se preporučuje model reosiguranja društvenih zajednica od posljedica prirodih nepogoda, kao svojevrsni finansijski instrument zaštite lokalnih i nacionalnih budžeta zajednice.

Rizici tehničke prirode nastaju zbog nesavršenosti projektovanja, izvodjenja, eksploatacije i održavanja elemenata sistema i spoznaja o njihovom stanju, te nestručnog ili neodgovornog rukovanja, a naročito:

- Prekomjerne eksploatacije energetskih transformatora
- Lošeg stanja razvodnih postrojenja i komandi
- Lošeg stanja relejne zaštite, elektroautomatike i telemehanike
- Lošeg stanja sistema pomoćnog napona i stanje akumulatorskih baterija
- Lošeg stanja stubova i ovjesne opreme nadzemnih vodova
- Lošeg stanja kablovskih vodova
- Lošeg stanja uredjaja za zaštitu od prenapona
- Neosposobljenost radnika za pripadajuće radno mjesto
- Neosposobljenost radnika za bezbjedan rad (rad na visini, rad sa opremom pod naponom...)
- Neosposobljenost radnika za sistem izvještavanja i kontrole

---

8 Rizik je funkcija vjerovatnoće pojave opasnosti, izloženosti (ukupna vrijednost svih elemenata u riziku) i ranjivosti (specifičnih uticaja na izlaganje).

[9] La Porte, T.R.: Critical Infrastructure in the Face of a Predatory Future: Preparing for untoward surprise, Vol. 15, No.1, 2007.

Ova grupa rizika najčešće i dovodi do prekida prenosa električne energije do krajnjih korisnika, ali je odlikuje kratkoća trajnja prekida i relativno mali uticaj po lokalno stanovništvo, ukoliko su osposobljene stručne servisne službe za brzo otklanjanje kvarova tehničke prirode. Pravilnim održavanjem opreme i redovnom kontrolom, mnogi od ovih rizika se mogu preventivno prepoznati i sanirati, najčešće i prije negó što dovedu do kvara na postrojenju ili mreži. Također, redovnom obukom operatera i stručnih službi, a posebno sa aspekta zaštite na radu, smanjuje se nivo rizika i posljedica po živote i zdravlje ljudi, pogotovo operatera koji su u stalnom kontaktu sa visokonaponskom mrežom.
Rizici iz grupe opšte bezbednosti mogu biti uzrokovani:

- Terorizmom i sabotažom
- Virtualnim napadom na računske centre
- Ratnim sukobom

Ovu grupu rizika prate velika razaranja imovine, duži prekidi elektrodistributivne mreže i veliki uticaj na ljude, ekonomski i društvenopolitički poredak. Poseban aspekt uticaja, uzrokovanih rizicima iz grupe opšte bezbjednosti, ogleda se u njihovom psihološkom uticaju, jer rizici iz ove grupe najčešće izazivaju strah i paniku kod stanovništva. Iz tog razloga se preporučuje izgradnja preventivnog sistema zaštite, koji obuhvata izradu kvalitetnih procjena ugroženosti i planova postupanja u slučajevima ekstremnih prekida napajanja i distribucije električne energije stanovništvu, te preventivno jačanje svijesti lokalnog stanovništva i njegova psihološka "priprema" za mogućnost ovakvog scenarija.
Akvizicijom podataka o različitim aspektima rizika, moguće je dobro estimirati različite nivoe rizika, koji se mogu javiti kao posljedica bilo tehničkih nepravilnosti koje utiču na stanje pouzdanosti i na gubitke električne energije, bilo društveno neprihvatljivog ponašanja i nasrtaja na imovinu ili elemantarnih nepogoda, te koji kao takvi direktno utiču na nivo pouzdanosti rada elektrodistributivnog sistema. Poduzimanjem preventivnih aktivnosti i izgradnjom sistema integrisane zaštite, biće znatno smanjene potencijalne štete, a u nekim slučajevima i izbjegnute u potpunosti, te neće imati nikakav uticaj na živote i zdravlje ljudi, ekonomski i društvenopolitički poredak društva.

INTEGRISANI SISTEM UPRAVLJANJA RIZICIMA I INTEGRISANE MJERE ZAŠTITE I SPAŠAVANJA NA KRITIČNOJ INFRASTRUKTURI

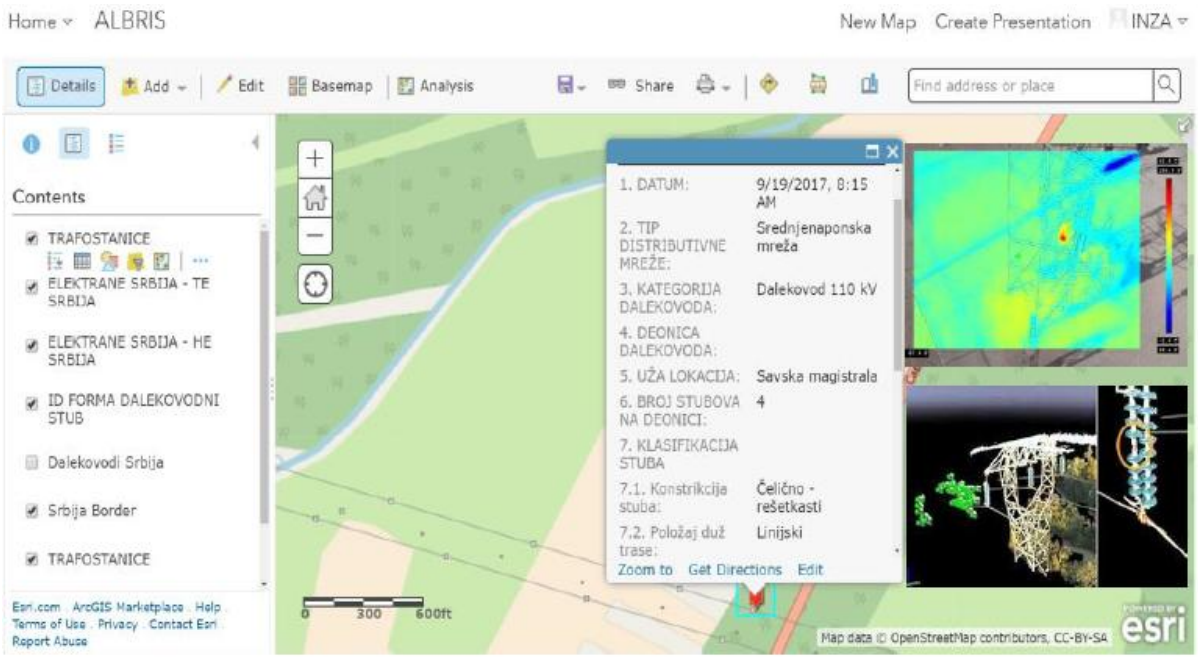
Zbog svoje važnosti po normalno funkcionisanje jednog društva u cjelini, te zbog kompleksnosti tehničko-tehnološkog procesa koji uglavnom prati normalan rad svakog sistema kritične infrastrukture, bilo da se radi o saobraćajnoj, energetskoj ili telekomunkacionoj mreži, odnosno lanaca snadbjevanja hranom i vodom, veoma je važno pravilno definisati pojmove integrisanog sistema upravljanja rizicima i integrisanih mjera zaštite i spašavanja. Integrisana zaštita je pojam koji je početkom 21. stoljeća uveden u opštu terminologiju struke, kao odgovor na sve učestalije i složenije rizike, te vrtoglavi progres inovacionih računarskih tehnologija i sistema. Gotovo da i ne postoji više neki složeniji tehničko-tehnološki proces, pogotovo kada je u pitanju kritična infrastruktura, a da nije upravljački automatizovan i povezan nekom softverskom platformom. Upravo razvoj računarsko-programske industrije, kao nezaobilaznog faktora u optimizaciji tehničko-tehnoloških procesa, doveo je i do inovativnog razmišljanja i razvoja integrisanih mjera zaštite i spašavanja kao odgovor na sve veću izloženost različitim vrstama rizika, bilo da su oni klimatski, tehnički ili opšti bezbjedonosni. Odgovor struke je bio sagledavanje stanja i davanje rješenja sistem integracije, koja po svojim karakteristikama može imati sledeće mjere zaštite: fizička, tehnička ili kombinovana fizičko-tehnička. Također integrisani sistem primjenjenih mjera zaštite i spašavanja možemo sagledati i kroz njegove komponente: prevencije, spremnosti i odgovora na aktuelne rizike. Za svaku od njih obrađujemo pojedinačno faze: identifikacije, analize i vrednovanja rezultata, kao posebnih procesa, koji strukturalno zavise jedan od drugog, te vode ka jedinstvenom integrisanom sistemu. Dakle nemoguće je kvalitetno odgovoriti na izazove, ukoliko ne sagledamo pravilno sve ove komponente i ne djelujemo integrisano u pravcu davanja optimalnih rješenja u cilju smanjenja potencijalnih rizika. Optimalni integrisani sistem zaštite i spašavanja podrazumjeva primjenu najčešće kombinovanih mjera zaštite, odnosno kombinaciju fizičke i tehničke zaštite kao najadekvatniji odgovor na izazove. Osposobljeno i utrenirano stručno osoblje uz primjenu tehničkih rješenja zaštite (alarmnih sistema, sistema videonadzora i kontrole pristupa), može adekvatno kontrolisati procese kako unutar samog sistema, tako i perimetrijsku zaštitu izvan tehnološkog procesa, odnosno, vršiti kontrolu neovlaštenog pristupa sistemu. Pri organizaciji ovih mjera, prije svega pri projektovanju, odabiru opreme i ugradnji iste, potrebno je voditi računa o izboru kvalitetnog tehničkog rješenja koje mora pratiti odgovarajuća tehnička oprema visoke kvalitete i otpornosti na specifične radne i klimatske uslove. Lica koja pružaju uslugu projektovanja, ugradnje i održavanja opreme moraju imati adekvatne strukovne

reference i zakonom definisane licence za obavljanje tih poslova. Također, ta lica moraju imati permanentni sistem treninga i vještine neophodne za brzu reakciju i pružanje pomoći unsrećenima (kurs prve pomoći, spasilački kurs i sl.). Obzirom da se radi o specifičnim sistemima kritične infrastrukture, čije nesmetano funkcionisanje je jedan od bitnih preduslova za stabilnost jednog društva u cjelini, primjena samo kompletno gore pobrojanih zahtjeva i uslova, garantuje optimalno funkcionisanje sistema integrisane zaštite i spašavanja.
Integrisano upravljanje rizicima svakim danom postaje nezaobilazni integracioni faktor svih tehničko-tehnoloških procesa i režima rada i poslovanja, bilo da se radi o javnom ili privatnom kapitalu. Da bi stručni pristup izgradnji sistema upravljanja rizicima dao najbolje rezultate, potrebno je početi isti sa izgradnjom sistema prevencije. Odnosno, izraditi kvalitetnu procjenu ugorženosti koja se mora bazirati na relevantnim informacijama, prikupljenim sistemski, putem identifikacionih formi u čijoj izradi se mora uvažiti i specifičnost tehnološkog procesa, odnosno iskustva i sugestije operativnog osoblja u samom procesu. Putem intervjua sa odgovornim licima i rukovaocima unutar sistema, potrebno je uočiti sve njihove potrebe i zahtjeve, koje treba ugraditi u identifikacione forme, te ih adekvatno tretirati u procesu analize podataka. Sam proces analize treba da poštuje domaću legislativu, ali i da prati Smjernice EU za izradu procjene ugoženosti SEC(2010) 1626 - od 2010, koje se baziraju na pristupu procjenjivanja u skladu sa standardom za upravljanje rizicima ISO 31001. Analiza podataka mora sadržavati matrice rizika i obavezna najmanje dva scenarija, najvjerovatniji i najgori mogući scenario. Preporučuje se i izrada SWOT analize snaga, slabosti, prilika i prijetnji, kao podloge za donošenje zaključaka i preporuka. Također, radi lakšeg prepoznavanja međusobno zavisnih procjena, potrebno je uraditi i dodatke u kojima se prepoznaje relevantni zakonski okvir, te uticaj na životnu sredinu, kao i eventualni prekogranični uticaj na druga područja. Vrednovanje podataka je kruna integrisanog sistema upravljanja rizicima, a pravilno upravljanje vrednovanjem može donijeti niz primarnih i sekundarnih benefita korisnicima ali i širem loklanom stanovništvu. Ovdje se prije svega misli na pravilnu klasifikaciju podataka pri čemu se mora uvažavati EUROSTAT klasifikacija i kategorizacija rizika po osnovu Smjernica EU i ISO 31001. Da bi lakše i pravilnije upravljali podacima, potrebno je izraditi odgovoarajuće baze na AutoCad i AutoDesk (CAD), Building Information Managment (BIM) i Geographical Information Sistem (GIS) platformama. Razvojem inovacionih tehnologija, struka je napredovala u fazi identifikacije rizika i prijetnji, pa tako danas imamo i savremene bespilotne letilice, s kojima možemo iz vazduha vršiti identifikaciju i nadzor potencijalnih rizika. Ako se ovome doda i da te letilice mogu biti opremljene specijalističkim kamerama visoke rezolucije (1mm/pix), te termografskim kamerama za snimanje energetskih gubitaka i toplote, onda možemo s pravom zaključiti da je razvoj visoke tehnologije olakšao i pojednostavio proces upravljanja rizicima, posebno na elektrodistributivnim mrežama i oobjektima proizvodnje i prenosa energije.
Da bi se sprovela adekvatna zaštita kritične elektrodistributivne infrastrukture od prirodnih i tehničko-tehnoloških nesreća i smanjenje rizika od katastrofa izazavanih klimatskim promenama, potrebno je izvršiti uspostavljanje interaktivnog rješenja za preventivno upravljanje rizicima i neregularnim radnim stanjima koja mogu poremetiti rad distributivnog sistema, putem IT georeferensirane programske platforme uz mogućnost kolektovanja relevantnih podataka sa terena u realnom vremenu (informacija, video i audio zapisa, slika i sl.). Uspostavljanje sistema integrisanog upravljanja rizicima i integrisanih mjera zaštite na elektrodistributivnoj mreži, treba da obezbjedi uslove i mogućnosti za dodatne akvizicije podataka, npr. o stanju elektrodistributivnog sistema i da formiranjem odgovarajuće baze podataka na osnovu ekspertske atributne liste podataka za svaki elemenat sistema (lista inspekcije elementa sistema), na osnovu čega će se moći izvršiti procena rizika i kreirati planove djelovanja u skladu sa svakim od njih. Potrebno je posebno izvršiti sagledavanje stanja:

- Čelično rešetkastih konstrukcija stubova nadzemnih vodova 35 kV i 10 kV;
- Izolatorske opreme i opreme za prihvatanje izolatorskog lanca na stubovima nadzemnih vodova;
- Provodnika - ugibi, vešanja, boja, deformacije pletenice, spojevi i električni mostovi;
- Koridora dalekovoda - prosečenost trase, izgrađenost objekata u koridoru dalekovoda;
- Ukrštanju svih nadzemnih distributivnih vodova i ukrštanja sa vodovima prenosne i nadzemnih mreža telekomunikacionih kablovskih operatora;
- Spojeva uzemljivača sa čelično rešetkastom konstrukcijom stuba;
- Temelja stubova;
- Očuvanosti strukture drvenih stubova;
- Građevinskog dela objekta transformatorskih stanica svih naponskih nivoa;
- Opomenskih tablica i drugih sigurnosnih elemenata koji moraju biti postavljeni na elektroenergetskiim objektima (stubovima, transformatorskim stanicama i dr.) u skladu sa propisom.

Specifičnosti grupe opštih bebjedonosnih rizika, u koje ubrajamo rizike od terorizma, sabotaže, virtualnih napada i ratova, obzirom da isti imaju razorne uticaje na društvo i ekonomiju, te da kao takvi proizvode psiholoških strah i osjećaj ugroženosti, zahtjevaju poseban i pažljiv pristup, kako u preventivnoj fazi, tako i u fazama

pripravnosti i odgovora. Integrisano upravljanje rizicima i primjena integrisanih mjera zaštite na kritičnoj infrastrukturi koja je izložena opštim bezbjedonosnim rizicima i prijetnjama, mora biti pod posebnom pažnjom državnog aparata i nacionalnih autoriteta, u smislu pažljivo odabranih kadrova, rješenja i partnera. Pozitivna iskustva iz inostranstva nam daju smjernice razvoja ovakvog integrisanog pristupa u pravcu pojačanog međusektorskog djelovanja institucija i odabira privatnog partnera u okviru modela javno-privatnog partnerstva. Ovaj model sistem integracije u upravljanju rizicima je naveden u članu 8. kao jedan od ključnih razloga za donošenje Evropske direktive za upravljanje rizicima na kritičnoj infrastrukturi:[10] *"S obzirom da razni sektori imaju vlastita iskustva, stručna znanja i zahtjeve koji se tiču zaštite kritične infrastrukture, potrebno je za Zajednicu razviti i provesti jedinstven pristup zaštiti kritične infrastrukture, uzimajući u obzir specifičnosti sektora i postojeće mjere koje se primjenjuju unutar pojedinih sektora, uključujući one koje već postoje na razini Zajednice ili na državnoj ili regionalnoj razini te, prema potrebi, važeće prekogranične sporazume o uzajamnoj pomoći između vlasnikâ/ operaterâ kritičnih infrastruktura. S obzirom na vrlo značajnu uključenost privatnog sektora u nadzor i upravljanje rizicima, planiranje poslovnog kontinuiteta i oporavak nakon nepogode, pristupom Zajednice trebalo bi se poticati potpuno uključivanje privatnog sektora".*Primjena integrisanih mjera zaštite i spašavanja u slučajevima ugrožavanja sigurnosti objekata i sistema kritične infrastrukture zahtjeva određeni stepen tajnosti, te primjenu inovativnih sistema rane identifikacije prijetnji, sistemske analize i subordinacije sa službama bezbjednosti, koje su posebno obučene, opremljene i pripremljene za suprostavljanje ovakvim vidovima prijetnji na kritičnoj infrastrukturi, koje po svom obimu, karakteru i posljedice, često mogu biti svrstavane i u nacionalne prijetnje.



ZAKLJUČAK

Klimatske promjene i globalne prijetnje od terorizma, predstavljaju najveće rizike po kritičnu infrastrukturu, a posebno po elektrodistributivnu mrežu, kao jednog od stubova razvoja i normalnog funkcionisanja lokalne zajednice. Tehnološki napredak i porast ovisnosti stanovništva o neprekidnom napajanju električnom energijom, obavezuju struku da izradi modele uspješnog i funkcionalnog odgovora izazovima u oblasti upravljanja rizicima. S tim u vezi Evropska Unija je dala preporuke za uspostavljanje sistema integrisanog upravljaja rizicima uključujući komponente identifikacije, analize i vrednovanja dobijenih rezultata. Primjena inovacionih tehnologija nam omogućava relevantan izvor prikupljanja komeptetnih podataka koji su iskoristivi u kasnijoj fazi analize i vrednovanja rezultata. Pravilna klasifikacija podataka i kategorizacija rizika nam daju pretpostavke za određivanje prioriteta djelovanja i primjene adekvatnih mjera u integrisanom sistemu zaštite i spašavanja. Upravljanje rizicima ne predstavlja više samo pojam prestižnosti i modernizacije procesa, već i sve prisutniju potrebu, kreiranu prema zahtjevu velikih sistema u kritičnoj infrastrukturi. Generalni zaključak možemo

[10] *DIREKTIVA VIJEĆA 2008/114/EZ od 8. decembra 2008. o utvrđivanju i označivanju evropske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite*

sublimirati predstavkom modela javno-privatnog partnerstva kao rješenja i adekvatnog odgovora sve prisutnijim izazovima i rizicima nastalim klimatskih promjena, globalizacijom i sve izrazitijim prijetnjama od terorističkih napada na sisteme kritične infrastrukture. Zato se izgradnja integrisanog sistema zaštite i spašavanja mora posmatrati kao investiranje u sistem preventivnog upravljanja rizicima u cilju smanjenja istih i jačanja kapaciteta pripravnosti i odgovora na sve izazove. Pravilnim investiranjem u prevenciju smanjujemo direktne i indirektne štete prema algoritmu 1:7:40[11] sa čime stvaramo preduslove za neometano funkcionisanje sistema kritične infrastrukture, a posebno kontinuiranog snadbjevanja stanovništva električnom energijom kao jednim od najpotrebnijih resursa čovječanstva.

LITERATURA

1. Čaleta D., 2011., "Counter Terrorism challenges", "Critical infrastructure protection",
2. Čaleta D., Shemella P., 2014., 1997, "Intelligence challenges",
3. Tomić D., 2017., "Terorizam",
4. Tomić D., Šećerov P., Garaplija E., 2018., "Menadžment kritične infrastrukture"
5. INZA Group, 2017., "Procjena ugroženosti za Brčko Distrikt BiH", "Prekida napajanja električnom energijom – Scenariji posljedica prekida od prirodnih nesreća i terorizma"

[11] *Kelman, I. and C.M. Shreve (ed.). 2014. Disaster Mitigation Saves. Version 6, 13 November 2014 (Version 1 was 30 October 2002). http://www.ilankelman.org/miscellany/MitigationSaves.doc*