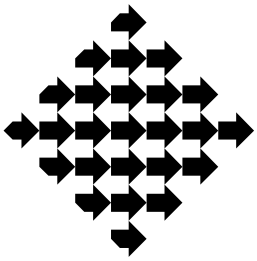
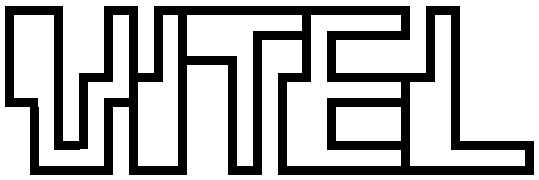
SLOVENSKO DRUŠTVO ZA ELEKTRONSKE KOMUNIKACIJE
ELEKTROTEHNIŠKA ZVEZA SLOVENIJE





Enaintrideseta delavnica o telekomunikacijah

KRITČNA INFRASTRUKTURA IN IKT

ZBORNIK REFERATOV

11. in 12. maja 2015 Brdo pri Kranju, Slovenija

31. delavnica o telekomunikacijah VITEL

ZBORNIK REFERATOV

31 Workshop on Telecommunications VITEL

PROCEEDINGS

Vsi referati v tem zborniku so recenzirani.
All papers in this proceedings have been peer reviewed.

Organizirata / *Organised by*:	Slovensko društvo za elektronske komunikacije
	Elektrotehniška zveza Slovenije
Pokrovitelj / *Sponsored by:*	IEEE Communications Society

Uredil / *Editor*:	Tomi Mlinar
Priprava za tisk / Prepress:	Tomi Mlinar
Naslovnica / Cover design:	Nikolaj Simič, Filip Samo Balan, Aleksander Vreže
Izdajatelj / Publisher:	Slovensko društvo za elektronske komunikacije
Tisk / Printing house:	Tidis, d. o. o.
Število izvodov / Copies:	100

ISSN 1581–6737

Kazalo prispevkov

Table of contents

11. 5. 2015

12. 5. 2015

Zgodovina delavnic o telekomunikacijah VITEL

History of Workshops on Telecommunications VITEL

1993: 1. *ISDN omrežja in storitve v Sloveniji*, Brdo pri Kranju
1994: 2. *Mobilne in brezvrvične telekomunikacije*, Brdo pri Kranju
1995: 3. *Podatkovna omrežja in storitve v Sloveniji*, Brdo pri Kranju
1995: 4. *Načrtovanje, upravljanje in vzdrževanje komunikacijskih omrežij*, Brdo pri Kranju
1997: 5. *Varnost in zaščita v telekomunikacijskih omrežjih*, Brdo pri Kranju
1997: 6. *Zbliževanje fiksnih in mobilnih omrežij ter storitev*, Brdo pri Kranju
1998: 7. *Telekomunikacije in sprejetje Slovenije v Evropsko unijo*, Brdo pri Kranju
1999: 8. *Omrežja IP, internet, intranet, ekstranet*, Brdo pri Kranju
1999: 9. *Upravljanje omrežij in storitev*, Brdo pri Kranju
2000: 10. *Mobilnost v telekomunikacijah*, Brdo pri Kranju
2001: 11. *Dostop do telekomunikacijskih storitev*, Brdo pri Kranju
2002: 12. *Poslovne telekomunikacije*, Ljubljana
2002: 13. *Kakovost storitev*, Brdo pri Kranju
2003: 14. *Varnost v telekomunikacijskih sistemih*, Brdo pri Kranju
2003: 15. *Mobilni internet*, Brdo pri Kranju
2004: 16. *Pametne stavbe*, Brdo pri Kranju
2005: 17. *Telefonija IP (VoIP)*, Brdo pri Kranju
2005: 18. *Storitev trojček = Triple play*, Ljubljana
2007: 19. *Brezžični širokopasovni dostop*, Brdo pri Kranju
2007: 20. *Optična dostopovna omrežja*, Brdo pri Kranju
2008: 21. *Povsem IP–omrežja*, Brdo pri Kranju
2009: 22. *Širokopasovna mobilna omrežja*, Brdo pri Kranju
2009: 23. *Konvergenčne storitve v mobilnih in fiksnih omrežjih*, Brdo pri Kranju
2010: 24. *Prehod na IPv6*, Brdo pri Kranju
2011: 25. *Internet stvari*, Brdo pri Kranju
2011: 26. *Komunikacije in računalništvo v oblaku*, Brdo pri Kranju
2012: 27. *Telekomunikacije in zasebnost*, Brdo pri Kranju
2012: 28. *Pametna mesta*, Brdo pri Kranju
2013: 29. *Infrastruktura za izpolnitev digitalne agende in kaj po tem – primer Slovenije;* Brdo pri Kranju
2014: 30. *Omrežja prihodnosti,* Brdo pri Kranju

Zgodovina mednarodnih simpozijev VITEL

History of International Telecommunication Symposium VITEL

1992: *VITEL*, Ljubljana
1994: *Subscriber Access*, Ljubljana
1996: *Broadband Communications Prospects and Applications*, Ljubljana
1998: *Mobility and Convergence Communication Technologies*, Ljubljana
2000: *Technologies and Communication Services for the Online Society*, Ljubljana
2002: *NGN and Beyond*, Portorož
2004: *Next Generation User*, Maribor
2006: *Content and Networking*, Ljubljana
2008: *DVB–T and MPEG4*, Bled
2010: *Digital Television Switchover Process*, Brdo pri Kranju

Uvodnik

Foreword

Kritična infrastruktura na področju informatike in komunikacij je … Če dobro pomislimo in smo iskreni, ne vemo natančno. Z vsakim odgovorom se nam odpirajo nova vprašanja, ki kažejo na vso širino in kompleksnost problematike. Ali se smemo osredotočiti zgolj na infrastrukturo? Kaj nam prinašajo nove tehnologije, koliko jih sploh še razumemo in obvladujemo? Kako na kakovost storitev, še zlasti v izrednih razmerah in ob velikih naravnih in drugih nesrečah, vpliva politika zniževanja stroškov, tako imenovani »sinergijski učinki« in racionalizacije? Ali se z povečevanjem odvisnosti od informacijskih in komunikacijskih storitev povečuje pomen tovrstne kritične infrastrukture in kako to posledično vpliva na nacionalno varnost v širšem smislu?

Družba postaja vedno bolj odvisna od informacijskih in komunikacijskih sistemov, ki postajajo vse kompleksnejši in zato vedno bolj nepredvidljivi. Navezanost ljudi na mobilne telefone, računalnike, tablice je postala že tako velika, da si brez njih ne morejo več zamisliti normalnega življenja. Ali gre za resnične ali zgolj namišljene človeške potrebe, je odvisno od dojemanja vsakega posameznika. Kljub temu lahko z gotovostjo trdimo, da nas trendi razvoja v želji po ustvarjanju novega, če tudi zgolj navidezno novega, silijo v vse večjo odvisnost.

Pojmovanje kritične infrastrukture se s časom spreminja. Uvodna predavanja bodo osvetlila pojma »kritična infrastruktura« in »evropska kritična infrastruktura«. Nekoč je bila kritična infrastruktura pomembna z vojaškega in ekonomskega stališča, danes se krog širi, zato nekateri celo menijo, da je prisotna v vseh sektorjih in celo v sami družbi. Tradicionalnim kritičnim infrastrukturam, kot so infrastrukture za preskrbo z vodo, električno energijo, transportni, finančni in bančni sistemi, se je pridružila informacijsko-komunikacijska infrastruktura. S tem so informatika in komunikacije presegle tradicionalno podporno vlogo in postale eden od ustvarjalcev družbenih odnosov in razvoja, ob tem pa žal tudi potencialni vir ogrožanja. Samo z ustreznimi merili lahko določimo, katera infrastruktura je kritična, oziroma bi v prihodnje lahko to postala. Nič manj pomembno ni vprašanje, kdo in kako naj gradi kritično infrastrukturo ter na kakšen način. Če je bila v preteklosti pretežno v državni lasti, se danes delež kritične infrastrukture v zasebni lasti stalno povečuje, kar še zlasti velja za področje informatike in komunikacij. Tako eno kot drugo ima svoje prednosti in slabosti, zato je prav, da jih vsaj grobo osvetlimo. Ne smemo prezreti tudi naravnih vplivov na delovanje komunikacijskih sistemov, kot je na primer vpliv zemeljskega magnetnega polja ob sončnih nevihtah ali posrednih vplivov v času velikih naravnih in drugih nesreč, kot je bila ujma z žledom v letu 2014. Pri tem je še kako pomembno, katere tehnologije uporabljamo in predvsem kako, da ne zmanjšamo že dosežene kakovosti storitev. To še zlasti velja za profesionalne in javne komunikacijske sisteme, ko ti zagotavljajo tudi profesionalne storitve. Na delavnici bomo nakazali, katere tehnologije uporabiti in kako se pripraviti za nemoteno delovanje tako javnih kot namenskih komunikacijskih sistemov.

Pomena kritične informacijsko-komunikacijske infrastrukture se zavemo šele, ko gre kaj narobe. Informacijski napadi na kritično infrastrukturo, vdori v omrežja in prisluškovanje, tudi na fizični optični infrastrukturi, nemoteno zagotavljanje storitev še zlasti v času izrednih razmer ali velikih naravnih in drugih nesreč je le nekaj vprašanj, na katera bomo poskušali odgovoriti na okrogli mizi »Varnostne grožnje v kritični infrastrukturi in njihove posledice na varnost države«

Za popotnico 31. delavnici VITEL tale misel: »Naj se sliši glas stroke in razuma, ne ideologije.«

Brdo pri Kranju, 11. maja 2015

Boštjan Tavčar
predsednik programskega odbora

Programski in organizacijski odbor delavnice

Programme and Organizing Committee

Programski odbor delavnice

Programme Committee

Boštjan Tavčar, predsednik
Alojz Hudobivnik
Ana Robnik
Marko Podberščič
Marko Jagodič

Organizacijski odbor delavnice

Organizing Committee

Nikolaj Simič, predsednik
Ivica Kranjčevič
Tomi Mlinar
Aleksander Vreže
Pavel Meše

Kritična infrastruktura in IKT

Iztok Prezelj in Uroš Svete, Obramboslovni raziskovalni center, Univerza v Ljubljani

Povzetek — Kritična infrastruktura odraža družbeno odvisnost od sodobnih tehnoloških omrežij. IKT je ena od ključnih kritičnih infrastruktur v sodobnih državah in v Sloveniji, saj bi njeno nedelovanje povzročilo veliko družbeno škodo. Tekst opredeli kritično infrastrukturo, evropsko kritično infrastrukturo in soodvisnost med kritičnimi infrastrukturami. Avtorja tudi orišeta pomen IKT v širokem spektru sodobnih kritičnih infrastruktur.

Ključne besede — kritična infrastruktura, evropska kritična infrastruktura, soodvisnost, IKT

Abstract — Critical infrastructure reflects high societal dependence from modern technological networks. ICT represents one of the key critical infrastructures in modern countries and in Slovenia due to high societal consequences in case of its malfunction. This text defines critical infrastructure, European critical infrastructure and cross-sectoral infrastructural dependence. Authors also describe the importance of ICT in the broad spectrum of modern critical infrastructures.

Keywords — critical infrastructure, European critical infrastructure, interdependency, ICT

I. UVOD

Pojmovanje kritične infrastrukture se je skozi čas spremenilo zaradi razvoja tehnologije in vzpona terorizma kot globalno pomembne grožnje varnosti. Nekoč se je med kritično infrastrukturo uvrščalo tiste infrastrukture, katerih daljše motenje bi lahko povzročilo večje vojaške in ekonomske posledice [3,8], danes pa govorimo o vseh infrastrukturah, na katerih temelji sodobni način življenja. Sem sodijo predvsem transportni sistemi (cestni, zračni, pomorski in železniški), telekomunikacijski in informacijski sistemi, elektroenergetski sistemi (elektrika, nafta, plin), finančni in bančni sistemi, sistemi preskrbe z vodo, sistemi preskrbe s hrano itd. Nekatere države pod kritično infrastrukturo uvrščajo tudi državne institucije, reševalne službe (vključno z javnim zdravstvom), kemično industrijo, in celo nacionalne spomenike ipd.

Kritičnost pri infrastrukturi pomeni nujnost in nepogrešljivost za delovanje sodobnih družb [14]. Kritična infrastruktura se tako nanaša na tisto infrastrukturo, katere motenje bi lahko imelo resne posledice za javnost [19]. Zaradi nevarnosti, da bi se kar vso infrastrukturo označilo kot kritično [glej 8] in ker enostavno ni mogoče ščititi in varovati vse infrastrukture, se sodobne države osredotočajo le na izbrane objekte, točke ali procese.

Grožnje kritični infrastrukturi so lahko številne. Znanost in stroka se osredotočata predvsem na naslednje kategorije:

- napake (povzročene predvsem zaradi pomanjkljivosti v sistemu, kar pomeni, da nastanejo predvsem zaradi notranjih vzrokov),
- nesreče (širok spekter bolj ali manj naključnih dogodkov, ki ponavadi nastanejo zunaj proučevanih ali prizadetih sistemov),
- napadi, ki so namerna dejanja, večinoma zunanjih akterjev [glej 10].

Dejstvo je, da se v sodobnem času o kritični infrastrukturi govori predvsem v luči potencialnih terorističnih groženj. Številni znani napadi so bili hkrati napadi na ljudi in na kritično infrastrukturo. Denimo napad 11. septembra 2001 je bil napad na vojaško in finančno infrastrukturo ter poskus napada na politično infrastrukturo (Senat ali Bela hiša). Boin, Lagadec, Michel-Kerjan in Overdijk [1] ugotavljajo, da je problem v tem, da teroristi lahko poskušajo izkoristiti našo (družbeno) odvisnost od kritične infrastrukture oziroma mreže. V tem smislu teroristom sploh ni treba uničiti določene mreže, ampak jo lahko uporabijo kot orožje proti družbi ali državi.

Zaščita kritične infrastrukture obsega aktivnosti za zaščito kritične infrastrukture pred potencialnimi in dejanskimi grožnjami. Zaščita kritične infrastrukture tako zajema koncepte, politike, strategije, pripravljenost v smeri preprečevanja destabiliziranja in odzivanje na destabilizacijske pojave pri delovanju mrež oziroma sistemov kritičnih infrastruktur (motnje, nesreče, napade ipd.). Zaščito kritične infrastrukture lahko opazujemo na več nivojih: v okviru tehničnega sistema, v okviru institucije (npr. podjetja), v okviru infrastrukturnega sektorja, na nacionalni ravni (vsi sektorji skupaj s perspektive sistema sistemov) in na mednarodni ravni (npr. v EU). Primarni cilj zaščite je preprečiti nastanek motenj ali jih odpraviti, ko se pojavijo. Mnogokrat pa se tudi govori o celovitem pristopu k zaščiti kritične infrastrukture, kar predvsem pomeni, da morajo države razviti integralen medsektorski in medorganizacijski pristop (npr. javno-zasebno partnerstvo).

II. EVROPSKA KRITIČNA INFRASTRUKTURA

Zadnji večji teroristični napadi v državah EU so vključevali tudi kritično infrastrukturo, ki je bila zaradi tega onemogočena. To je poleg nekaterih nesreč in dogodkov, ki so dobili evropske razsežnosti, ključni razlog za začetek razmišljanja o evropski kritični infrastrukturi. Evropski svet je tako leta 2004 zaprosil Evropsko komisijo, naj pripravi celovito strategijo za varovanje kritične infrastrukture. Komisija je oktobra 2004 sprejela Sporočilo o varovanju kritične infrastrukture v boju proti terorizmu, v katerem je dala jasne predloge glede okrepitve preprečevanja terorističnih napadov na kritično infrastrukturo in s tem povezano pripravljenostjo v Evropi. Svet je v sklepih o »preprečevanju, pripravljenosti in odzivu na teroristične napade« in v »Solidarnostnem programu EU o posledicah terorističnih groženj in napadov« podprl namero Komisije, da predlaga Evropski program za varovanje kritične infrastrukture (EPCIP). Komisija je novembra 2005 sprejela Zeleno knjigo o evropskem programu za varovanje kritične infrastrukture, v kateri so bile določene politične možnosti, kako bo Komisija vzpostavila EPCIP [glej 6]. Komisija je decembra 2006 prvič predlagala direktivo Sveta o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njenega varovanja. Ta predlog direktive je predstavil ukrepe glede ugotavljanja in določanja

evropske kritične infrastrukture (EKI) ter oceno potrebe za izboljšanje njene zaščite in varovanja [glej 15, 16]. Ratifikacija evropske direktive se je zapletla zaradi nesoglasij med državami glede lastne EKI [18].[1] Na koncu izjemno zahtevnega procesa usklajevanja je bila vendarle sprejeta okrnjena direktiva, ki danes predstavlja prvi korak v postopnem pristopu za ugotavljanje in določanje EKI. Sama direktiva je usmerjena zgolj na energetski in prometni sektor, medtem ko so drugi sektorji za zdaj izpuščeni. To pomeni, da so morale vse države določiti objekte EKI v podsektorju energetike, nafte, plina, cestnega, železniškega, zračnega in vodnega prometa. Države članice in lastniki oziroma upravljavci te infrastrukture morajo imeti varnostne načrte, varnostne uradnike, kontaktno točko z EU, poleg tega pa morajo tudi ocenjevati tveganja, grožnje in ranljivosti [2]. Iz razprav pri sprejemanju direktive je razvidno, da se bo v prihodnosti posebno pozornost namenilo predvsem sektorju informacijske in komunikacijske tehnologije.

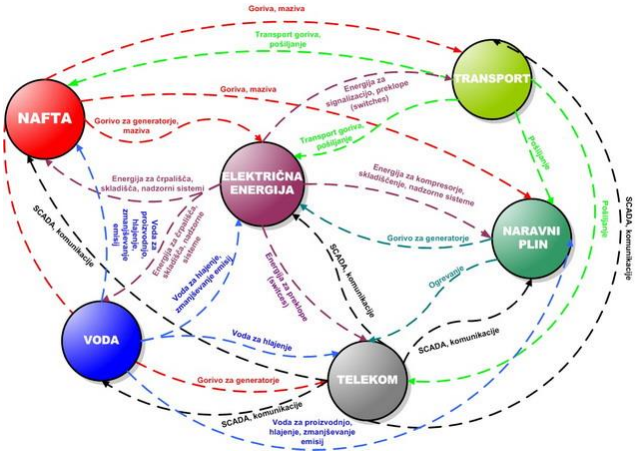
III. SOODVİSNOST MED KRİTİČNİMİ İNFRASTRUKTURAMİ

Sektorji so med seboj funkcionalno soodvisni, kar pomeni, da je funkcionalnost enega sektorja ali sistema odvisna od funkcionalnosti drugih. Motnje v enem sektorju lahko povzročijo motnje v drugih sektorjih. Boin, Lagadec, Michel-Kerjan in Overdijk [1] ter Perenboom [13] razumejo naraščajočo soodvisnost med sektorji kot soodvisnost med mrežami. Razlog temu so našli v tržnih mehanizmih, ki zahtevajo od mrež večjo zmogljivost oziroma učinkovitost, kar je pripeljalo do večje vključitve nove in sodobne tehnologije. Večja učinkovitost je izgrajena na boljši povezanosti, kar pomeni večji soodvisnosti, ki povratno zahteva še večjo zmogljivost. Tako se zdi, da bodo lahko vedno manjše motnje povzročale vedno večje učinke.

Le Grand, Springinsfeld in Riguidel [10] na tej točki poudarjajo razliko med odvisnostjo in soodvisnostjo. Odvisnost pomeni, da stanje ene infrastrukture vpliva na stanje druge, medtem ko je soodvisnost odvisnost v obe smeri. V določenih primerih govorimo torej tudi o soodvisnosti. Hellstrom [8] v zvezi s tem ugotavlja, da do škodljivih prenosov lahko prihaja tudi, če sistemi med seboj niso fizično povezani. Vzajemna povezanost je lahko relevantna samo v določenih primerih oziroma pod določenimi pogoji. Slika 1 prikazuje ilustrativno oblike soodvisnosti med sektorji.

Nekateri drugi avtorji [npr. 11] ugotavljajo, da obstaja hierarhija odvisnosti med sektorji, kar pomeni, da so eni bolj odvisni od drugih. V tem smislu lahko ugotovimo lahko dokaj veliko centralnost elektroenergetskega sektorja, saj so vsi drugi sektorji odvisni od električne energije. Zadnje večje zatemnitve po Evropi so povzročile motnje denimo v delovanju mobilne telefonije, ne pa tudi stacionarne telefonije. Za primer naraščajoče soodvisnosti pa lahko vzamemo vedno večjo odvisnost kritičnih infrastruktur od informacijskih in komunikacijskih sistemov. To soodvisnost lahko razumemo tudi v negativnem smislu, saj bi se funkcionalne motnje iz enega sektorja ali sistema lahko hitro prenesle na druge.

[1] Nesoglasja so se še najbolj videla med velikimi in majhnimi državami, ki se niso mogle sporazumeti o kriterijih v zvezi z višino škode. Določena višina škode v primeru nedelovanja določene infrastrukture v veliki državi bi se komaj poznala, medtem ko bi v mali državi prišlo že do nacionalne katastrofe.



Slika 1: Ilustrativna slika soodvisnosti med infrastrukturami [13]

Obstaja več splošnih kategorij soodvisnosti:

- fizična soodvisnost (npr. materialni output ene infrastrukture se uporablja s strani druge infrastrukture),
- kibernetska odvisnost (npr. infrastrukture so odvisne od informacij, ki prihajajo po informacijski infrastrukturi),
- geografska soodvisnost (npr. infrastrukture se nahajajo na skupnem prostoru),
- logične soodvisnosti (npr. infrastrukture so povezane prek finančnih trgov) [13, 10].

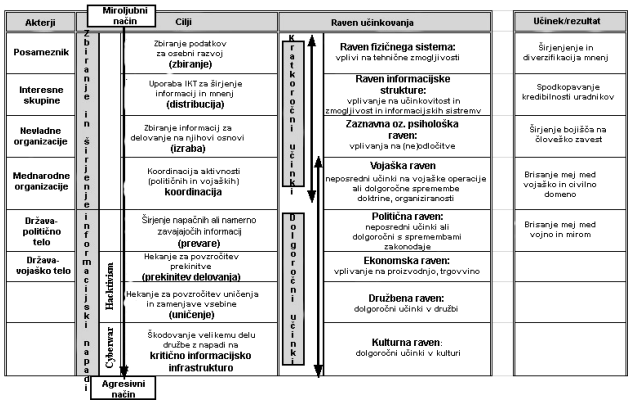
IV. INFORMACIJSKO-KOMUNIKACIJSKA TEHNOLOGIJA KOT KRITIČNA INFRASTRUKURA

Razprava o kritični infrastrukturi in informacijsko-komunikacijski tehnologiji (IKT) odraža vso kompleksnost sodobnih družb, tako kar zadeva dejanske procese, še bolj pa kar zadeva znanstveno preučevanje le-teh. Vsekakor je nesporno dejstvo, da je razvoj predvsem digitalne IKT v zadnjih nekaj desetletjih prinesel izredne spremembe v praktično vseh pomembnih oz. kritičnih družbenih podsistemih kot so ekonomski, upravno-politični, medijski in ne nazadnje tudi nacionalnovarnostni, da ne omenjamo vseh ostalih podpornih procesov, ki omogočajo delovanje sodobnih družb.

Sodobna in tehnološko razvita država se danes tako sooča z največjimi strukturnimi spremembami od padca Berlinskega zidu in konca hladne vojne, ki se nanašajo na njeno gospodarsko, politično, informacijsko in ne nazadnje tudi varnostno vlogo. Zlasti slednja je za našo razpravo ključnega pomena, saj se je odnos do varnostnega vprašanja v zadnjih letih temeljito spremenil, po drugi strani pa je informacijska dimenzija postala eden ključnih virov družbene moči, o čemer več v nadaljevanju .

Čeprav so tehnološko-tehnične revolucije vedno v človeški zgodovini bile predmet tudi varnostnih razsežij, pa vendarle je le malo katera tako spremenila razmerja moči kot je to primer informacijsko-komunikacijske tehnologije (IKT) in z njo povezane informacijske revolucije. Pogosto sicer menimo, da je bilo obdobje hladne vojne zaznamovano predvsem z jedrsko oboroževalno tekmo ter bojem za vire v fizičnem (realnem) prostoru, vse več avtorjev vzroke za znan razplet tega obdobja ter prevlado zahodnega sveta išče tudi v razvoju informacijske tehnologije in njenem vplivu tako na oborožitvene sisteme kot načine delovanja vojaških in nevojaških organizacijskih struktur [22, 9]. Navkljub sicer različnim razlagam vzrokov in namenov, ki so na koncu privedli do predhodnika interneta ARPANET-a, obstaja

danes vse večje soglasje, da je razmah na internetnem protokolu temelječe informacijsko-komunikacijske tehnologije in nastanek kibernetskega prostora nedvomno v temeljih spremenil praktično vse družbene podsisteme kot tudi vlogo posameznika v njih. Kakorkoli torej ocenjujemo dogodke konec 50. in začetek 60. let prejšnjega stoletja, ki so privedli do informatizacije sveta, nobenega dvoma ni, kibernetski prostor in varnostni sektor sta povezana že od samega začetka tako v teoretično-konceptualnem kot empiričnem smislu, pri tem pa je njun odnos inverzno deduktiven. To pomeni, da se po eni strani (varnostna) teorija in konceptualizacija morata prilagajati razvoju tehnologije, po drugi strani pa velja tudi obratno. Koncepti, kako izkoristiti IKT kot sredstvo za spremembo strukture moči, seveda v veliki meri vplivajo, katera tehnološka sredstva bodo uporabljena in na kakšen način.



Slika 2: Varnostne implikacije uporabe informacijsko-komunikacijske tehnologije [po 4].

IKT se je v nekaj desetletjih razvila na strateško/globalno raven, kar potrjujejo tudi primeri iz številnih držav, pri čemer lahko v ta namen izpostavimo institucionalni razvoj nacionalnovarnostnih sistemov [glej 21], analizo medijskega poročanja o varnostnih incidentih ter ne nazadnje ugotovitve znanstveno-raziskovalne sfere. Večina informacijsko razvitih držav ima danes izdelano zaščito kritične (informacijske) infrastrukture, prav tako pa so v okviru nacionalnovarnostnih sistemov oblikovale nekatere nove institucije, katerih namen je zagotoviti varnost tudi informacijskega področja oz. preprečiti, da bi uporaba IKT postala grožnja nacionalni varnosti (kot je primer Zveznega urada za varnost informacijske tehnologije v Nemčiji (nem. Bundesamt für Sicherheit in der Informationstechnik). In končno, v razprave o informacijski grožnji nacionalni varnosti v sodobnih družbah se vse bolj dejavno vključuje tudi znanost, tako družboslovna kot naravoslovno-tehnična. Vsekakor lahko rečemo, da je omenjeno področje med tistimi, ki najbolj legitimizirajo interdisciplinarnost ter potrebo po enovitem in holističnem znanstvenem delovanju.

A. Vpliv uporabe informacijsko-komunikacijske tehnologije na (informacijsko) moč

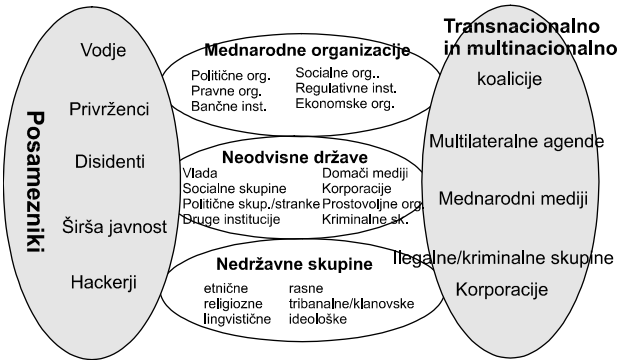
Informacijski vidik pridobivanja in uveljavljanja družbene moči se je še posebej spremenil na podlagi uporabe IKT, pri tem pa moramo najprej izpostaviti informacijske družbe. Kajti informacije niso zgolj multiplikator drugih virov moči (zlasti ekonomske, politične, medijske,…), temveč vir moči same po sebi [12]. Glede na dejstvo, da je IKT povzročila pravo revolucijo pri zbiranju, obdelavi in prenosu podatkov, je razumljiv tudi njen vpliv na družbeno, še zlasti pa na informacijsko moč, ki se je v času informacijske revolucije še povečal [7]. Spremenila so se namreč razmerja med posameznimi varnostnimi akterji, prav tako pa se je spremenil tudi način oblikovanja identitet teh akterjev. Vplive IKT lahko zaznamo pri večini oblik družbene moči, kar ima izjemen vpliv tudi na koncepcijo zaščite kritične infrastrukture. Po eni strani lahko **IKT preučujemo kot samostojni sektor, po drugi strani pa jo lahko preučujemo tudi znotrajsektorsko**.

Vpliv IKT na družbeno moč bomo predstavili v okviru njene instrumentalne oblike, ki se nanaša na sposobnost njenih nosilcev, da vplivajo na določene vidike medsebojnih odnosov v razmerju do drugih akterjev. Uporaba IKT (oz. katere koli druge tehnologije) je v tem okviru v prvi vrsti namenjena povečevanju teh sposobnosti. To pa je hkrati tudi najosnovnejša raven analize preučevanja odnosov med njeno uporabo in močjo. Povečala je namreč sposobnosti tradicionalnih globalnih akterjev, kot so države in multinacionalke, hkrati pa je povečala moč tudi drugim akterjem, transnacionalnim družbenim gibanjem (primer Wikileaks in Anonymous) in uporniškim oz. terorističnim skupinam (primer internetne aktivnosti Islamske države). IKT je namreč že zelo zgodaj postala izredno pomemben dejavnik in vir moči v državah s primerno razvito infrastrukturo. Tako je npr. Pentagon podpiral komunikacijsko družbo AT&T vse do njenega konca, trdeč, da gre za interes nacionalne varnosti. Sicer pa je informacijska in komunikacijska infrastruktura oz. tehnologija postala varnostno zanimiva že v 60. letih prejšnjega stoletja, ko so se nakazovale prve povezave z nacionalno močjo. Tako so se številne države (Japonska, Francija) začele zavedati, da bi imelo vsako zaostajanje v razvoju informacijske infrastrukture velike posledice tako za ekonomski sistem kot tudi sam položaj države v mednarodni skupnosti, prav tako pa so tudi v okviru mednarodnih organizacij, kot so Mednarodna telekomunikacijska zveza (ang. International Telecommunication Union – ITU) in Mednarodna banka za obnovo in razvoj (The International Bank for Reconstruction and Development – IBRD), IKT obravnavali kot enega pomembnejših virov za zmanjševanje zaostanka manj razvitih držav za razvitimi. Obravnavanje v luči instrumentalne moči je bilo sicer najočitnejše v 80. letih prejšnjega stoletja, ko so se vrstile debate o ekonomski konkurenčnosti. Primer Francije smo že omenili, debate pa so se odvijale v širšem evropskem prostoru, saj je Evropska komisija leta 1987 izdala zeleno in leta 1992 belo knjigo, ki sta izpostavljali pomen primerne informacijske avtoceste za evropsko industrijo. V Aziji pa so Japonska, Južna Koreja, Singapur in Indija sprožile pobudo za pospešitev razvoja informacijske infrastrukture. Take pobude so bile stalno prisotne tudi v ZDA, kajti uporaba IKT je doživela razmah izven vojaškega oz. nacionalnovarnostnega sistema ravno v tej državi. Celo za časa Reaganovega predsednikovanja, čigar administracija je prisegala na ekonomski liberalizem (laissez faire, so zvezne oblasti veliko napora vlagale v preprečevanje zmanjševanja ameriške konkurenčnosti na trgu polprevodnikov, kasneje pa je Clintonova administracija pod vodstvom podpredsednika Gora načrtno oblikovala nadaljnji razvoj nacionalne informacijske infrastrukture.

Instrumentalne zadeve o ekonomski moči in tehnologijah so se združile s tradicionalnimi, kot so varnost in politične spremembe, šele konec prejšnjega stoletja. Koncepti varnosti so se spremenili v dveh smereh.

Prvič, informacijske tehnologije so se uporabile za povečanje zmogljivosti pri reševanju različnih nalog, pri tem pa je njihova uporaba zajemala celoten spekter od t. i. pametnih orožij do organizacijskih sprememb na področju notranje varnosti, obveščevalne skupnosti ali oboroženih sil. Danes smo v razvoju tehnologije zlasti na področju umetne inteligence prišli celo tako daleč, da informatizacija oborožitvenih sistemov ne zadošča več, pač pa se odkrito govori o avtonomnih bojnih sistemih/robotih, ki bi v bližnji prihodnosti celo sami sprejemali odločitve in delovali brez človekovega nadzora.

In drugič, zaščita nacionalne kritične informacijske infrastrukture pred različnimi oblikami groženj (od individualnih hekerjev, ki pridobivajo zaupne podatke, do publicističnih primerov "kibernetske" vojne) je postala popolnoma regularna in legitimna naloga države [20]. Uporaba informacijskih mrež pa je postala tudi izredno pomemben dejavnik političnih sprememb, še zlasti po padcu železne zavese in odprtju nekdanjega socialističnega tabora novim informacijskim in komunikacijskim tehnologijam. V svetu, v katerem se je spremenil pomen zadrževanja, jedrskega dežnika ter konvencionalnega odvračanja, lahko informacijska prednost okrepi intelektualne povezave med zunanjo politiko ter vojaško močjo in tako nudi nove oblike ohranjanja položaja v zavezništvih in *ad hoc* koalicijah [Nye in Owens v 20] posebej ko gre za oblikovanje t.i. mehke pomoči (ang. soft power). Vendar pa IKT ni postala pomemben dejavnik moči nacionalne države šele s koncem hladne vojne, ampak ga je v določenem smislu celo povzročila. Informacijska revolucija je namreč naredila Sovjetsko zvezo za ekonomsko, politično ter celo vojaško poraženko, kajti povečala je ekonomski prepad med blokoma, ki se je nakazoval že v 80. letih prejšnjega stoletja, pri čemer so ZDA in njeni zavezniki v Evropi in Aziji prehiteli SZ v večini virov družbene moči [5]. Instrumentalne značilnosti IKT pa seveda segajo onstran države. Lahko bi celo rekli, da je IKT povzročila **demonopolizacijo države, kar zadeva varnostna prizadevanja, pa tudi ogrožanja.**



Slika 3: Sodobno (informacijsko) varnostno okolje

Proliferacija oz. širjenje uporabe informacijsko-komunikacijske tehnologije povsod po svetu je torej eden najpomembnejših dejavnikov, ki vplivajo na razmerja tako med državami samimi kot med njimi in drugimi akterji sodobnega varnostnega okolja, v katerem igrajo vse pomembnejšo vlogo tudi posamezniki, nevladne organizacije ter teroristične in druge uporniške skupine. Zato je njeno vlogo v konceptu instrumentalne moči nujno treba obravnavati preko okvirov države, čeprav imajo države in multinacionalke sicer boljši dostop do informacijske infrastrukture in informacij nasploh.

B. Raziskovanje IKT v okviru kritične infrastrukture v Sloveniji

Čeprav Slovenija, kar zadeva raziskovanje IKT v okviru kritične infrastrukture, ni popolnoma nepopisan list papirja (med leti 2006 in 2008 smo tudi na Obramboslovnem raziskovalnem centru izvajali Ciljni raziskovalni projekt Definicija in zaščita kritične infrastrukture v RS), pa so dejansko šele lanska ledena ujma ter razprave glede lastništva največjega telekomunikacijskega operaterja odprle vprašanja, ki bi najbrž že davno morala biti rešena. Predvsem gre za pristojnosti na področju zaščite kritične informacijske infrastrukture ter njenega vpliva na družbo kot tako. Ledena ujma, ki se je zgodila lani med koncem januarja in prvim tednom februarja 2014 ter nato takoj prešla v nekaterih delih tudi v poplave, je primer, ki je preprosto pokazal vso ranljivost sodobnih elektriziranih in tudi informatiziranih družb, prepletenost in soodvisnost ključne družbene infrastrukture [17], odvisnost od distribucije električne energije, šibkost informacijsko-komunikacijskih sistemov primeru ekstremnih naravnih pojavov (čeprav za nekatere, kot je internet, pogosto poudarjamo, da naj bi preživeli celo jedrski spopad), prav tako pa so številni deli države zaradi podrtega drevja in neprevoznih cest ostali »odrezani od sveta« in so morali dokazati, kaj v času globalizacije pomeni avtarkičnost v najbolj neugodnem letnem času. Lanska ledena ujma je bila gotovo največja grožnja slovenski družbi vse od nastanka samostojne države in vojne, ki je sledila. Pokazala je, da je IKT izredno ranljiva v primeru naravnih nesreč, po drugi strani pa državni oblasti ob prekinjenih fizičnih komunikacijah omogoča edini instrument za nadzor nad razmerami (ang. situation awareness). Glede na to, da večjih izpadov IKT, kot je bil primer Estonije v letu 2007, v Sloveniji na srečo še nismo imeli, je prav omenjena naravna nesreča ponovno vzbudila pozornost tako tehničnih kot družboslovnih disciplin, ki preučujejo varnostne pojave na informacijskem področju. Pokazala pa je še nekaj. V že omenjenem raziskovalnem projektu smo navkljub izhodiščem Evropske unije, ki je sektor informacijske infrastrukture razdelila na 6 podsektorjev (internet, zagotavljanje fiksnih telekomunikacij, zagotavljanje mobilnih telekomunikacij, radijske komunikacije, satelitska komunikacija, oddajniki) sami izhajali samo iz dveh podskupin (programje oz. programska oprema ter strojna oprema in komunikacije). Taka delitev se je kasneje pokazala kot mnogo bolj smiselna, saj je prišlo do sinergije telekomunikacij in interneta, po drugi strani pa smo želeli opozoriti, da ima tudi programska oprema za družbo zlasti zaradi izjemno kratkih razvojnih ciklov in pomanjkljivosti lahko zelo pomembne učinke in zato tudi spada v kritično infrastrukturo. Predvsem pa je programska oprema tista, ki daje podatkom uporabno vrednost, jih pretvarja v informacije ter omogoča moč na osnovi pravilnih odločitev.

Čeprav je omenjen raziskovalni projekt dal določene pozitivne rezultate, pa smo naleteli tudi na kar nekaj ovir ko gre za odnos države in zasebnih komercialnih akterjev na tem področju. Slednji v času, ko ni varnostnih incidentov, namreč naložbo v varnost pogosto jemljejo kot nepotreben strošek, še posebej če tovrstne ukrepe predpiše država. Javno-zasebno partnerstvo se v Sloveniji na tem področju ni razvilo. Prav tako pa se je pokazalo, da moramo podobne analize kritičnosti informacijsko-komunikacijske infrastrukure izvajati dvonivojsko. To pomeni, da je potrebno IKT preučevati kot samostojni sektor (v tem pogledu mora za

nadaljnje raziskovanje služiti naš podsektor, ki smo jo imenovali IKT komunikacije in strojna oprema), po drugi strani pa je potrebno IKT preučevati tudi znotraj posameznih sektorjev in podsektorjev. Predvsem pa se bomo morali v obdobju interneta reči (ang. Internet of Things) vse resneje ukvarjati tudi z vprašanjem, kakšne posledice v fizičnem okolju od ravni posameznika pa vse do državnih struktur bi povzročil morebiten izpad IKT.

V. ZAKLJUČEK

Kritično infrastrukturo sestavljajo kompleksni sociotehnični sistemi, med katerimi igra IKT izjemno pomembno vlogo. Izpad IKT bi povzročil veliko in tudi nepredvidljivo družbeno ter gospodarsko škodo. IKT je pronicala v vse druge (kritične) infrastrukture, zato bi njeno nedelovanje ali onesposobitev povzročila medsektorsko škodo. Kritičnosti IKT zaradi prepletenosti tehnologij praktično ni več mogoče obravnavati sektorsko, to je s strani zgolj ene nacionalne institucije. Tako morajo sodobne države oblikovati integralno politiko zaščite kritične infrastrukture, ki vključuje tudi področje IKT. Pri zaščiti se je načeloma treba osredotočati le na najbolj ogrožene in ranljive dele infrastrukture. Ogroženost in ranljivost pa se lahko določi s številnimi metodologijami. Sloveniji želiva veliko modrosti in čim manj medinstitucionalnih konfliktov pri urejanju tega področja v prihodnosti.

LITERATURA

[1] Boin, Arjen, Lagadec, Patrick, Michel-Kerjan, Erwann in Overdijk, Werner (2003): Critical Infrastructures under Threat: Learning from the Antrax Scare. Journal of Contingencies and Crisis Management (let. 11, št. 3): 99–104.

[2] Council Directive on the Identification and Designation of European Critical infrastructures and the Assessment of the Need to Improve their Protection (2008), 8.12., Official journal of the EU, 23.12., Brussels.

[3] Dunn, M. (2005) The socio-political dimensions of critical information infrastructure protection. *International Journal of Critical Infrastructures* 1(2/3): 258 –

[4] Dunn, M. 2001. The Cyberspace Dimension in Armed Conflict: Approaching a Complex Issue with Assistance of the Morphological Method. Information & Security, 7, 145-158.

[5] Gompert David C. (1998). National securitiy in the information age, Naval war college review, vol. 51, br. 4.

[6] Green Paper on a European Programme for Critical Infrastructure Protection (2005), EC, 17.11., Brussels.

[7] Groß, Jürgen, *Militär und Macht im internationalen System*, Das Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg, Hamburg, 2003.

[8] Hellstrom, Tomas (2006): Critical Infrastructure and Systemic Vulnerability: Towards a Planning Framework. Research paper, Safety Science.

[9] Klimburg, Alexander. 2011. Mobilising Cyber Power. Survival 53(1), str. 41-60.

[10] Le Grand, Gwendal, Springinsfeld, Franck in Riguidel, Michel (2003): Policy Based Management for Critical Infrastructure Protection. Research report, ACIP Project, funded by the European Commission.

[11] Lewis, Ted (2006): Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. New Jersey: Wiley Interscience.

[12] Mayer-Schönberger Viktor, Gernot Brodnig. 2001. Information power: international affairs in the cyber age. Harvard University, Harvard.

[13] Peerenboom, James (2001): Infrastructure Interdependencies: Overwies of Concepts and Terminology. Research paper, Infrastructure Assurance Center, Argonne.

[14] Pommerening, Christine (2004): A Comparison of Critical Information Infrastructure Protection in the US and Germany: An Institutional Perspective, Conference Paper – American Political Science Association, Annual Meeting - Chicago.

[15] Predlog Direktive o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njenega varovanja (2008), Svet EU, Bruselj, 22. 5.

[16] Predlog direktive Sveta o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njenega varovanja (2006), Svet EU, Bruselj, 18. 12.

[17] Prezelj, Iztok, Kopač, Erik, Svete, Uroš, Žiberna, Aleš. Cross-sectoral scanning of critical infrastructures : from functional differences to policy-relevant similarities. *Journal of homeland security and emergency management*, ISSN 1547-7355, 2012, vol. 9, iss. 1, graf. prikazi, doi: 10.1515/1547−7355.1901.

[18] Prezelj, Iztok. Nacionalna kritična infrastruktura v Republiki Sloveniji. Teorija in praksa, , jul.-avg. 2009, letn. 46, št. 4, str. 464-484.

[19] Reinermann, Dirk in Weber, Joachim (2003): Analysis of Critical Infrastructures: the ACIS Methodology. Federal Office for Information Security, Bonn, Germany.

[20] Rosenau, James N., J. P. Singh. 2002. Information technologies and global politics: the changing scope of power and governance. Albany: state university of New York press.

[21] Svete, Uroš. European e-readiness? Cyber dimension of national security policies. Journal of comparative politics, ISSN 1338-1385. [Online ed.], Jan. 2012, vol. 5, no. 1, str. 38-59. http://www.jofcp.org/assets/jcp/JCP-January-2012.pdf.

[22] Štrubej, Janez. 2008. Hladna vojna in bitka za informacijsko tehnologijo. Ljubljana:Pasadena.

Iztok Prezelj (iztok.prezelj@fdv.uni-lj.si) je doktor obramboslovnih znanosti in izredni profesor na Fakulteti za družbene vede pri Univerzi v Ljubljani. Raziskovalno dejavnost opravlja na Obramboslovnem raziskovalnem centru in pedagoško dejavnost na Katedri za obramboslovje. Njegovo raziskovalna dejavnost zajema področja nacionalne varnosti, ocenjevanja ogrožanja, kriznega menedžmenta, terorizma, obveščevalne dejavnosti in kritične infrastrukture. V obdobju 2006-2008 je vodil prvi znanstveni projekt v Sloveniji na temo kritične infrastrukture. Avtor je član različnih strokovnih združenj, med drugim tudi Evropske ekspertne mreže o terorizmu (European Expert Network on Terrorism Issues). Med drugim predava predmete, kot so Krizni menedžment in sodobna varnost, Sodobni terorizem in sistemski protiukrepi, Sodobni obveščevalni sistemi itd.

Uroš Svete (uros.svete@fdv.uni-lj.si) je diplomiran politolog smeri obramboslovje ter doktor obramboslovja. Svoje raziskovanje zadnjih 15 let usmerja v varnostne implikacije informacijsko-komunikacijske tehnologije ter preučevanje sodobnih asimetričnih konfliktov. Leta 2002 je zagovarjal magistrsko delo z naslovom Vloga in pomen informacijske tehnologije v sodobnem asimetričnem vojskovanju, leta 2005 pa doktorsko disertacijo (Varnostne implikacije informacijsko-komunikacijske tehnologije). Od leta 2000 je zaposlen na Katedri za obramboslovje na Fakulteti za družbene vede, kjer je trenutno docent in njen predstojnik. Na prvi in drugi stopnji študijskega programa obramboslovje med drugim predava tudi predmeta Informatizacija sodobnih oboroženih sil in Informacijska tehnologija in nacionalna varnost. Mednarodno je aktiven v okviru Svetovne sociološke zveze (ISA) - raziskovalnega odbora Armed Forces and Conflict Resolution, ki je največje svetovno združenje vojaških sociologov, kjer opravlja naloge izvršnega sekretarja.

Identifikacija kritične infrastrukture

Katja Kmet in Albin Poljanec, Agencija za komunikacijska omrežja in storitve RS, Ljubljana

Povzetek — Pričujoči članek je poskus identifikacije kritične infrastrukture, ki je ključna za delovanje elektronskih komunikacijskih storitev. Prispevek je zgolj poskus, torej nima ambicij konkretne določitve storitev in posledično infrastrukture, izpad katere bi lahko ogrozil ključne funkcije za delovanje države. Odgovor na to vprašanje bodo dali uporabniki, pravzaprav ga bo morala dati država sama, ko bo določila kritične dele omrežja in njegove elemente ter sprejela odločitev v kolikšni meri in na kakšen način naj jih zaščiti. V nadaljevanju bo predstavljena zakonodaja v zvezi s kritično infrastrukturo in pogled regulatorja nanjo. Zaključujemo pa z izzivi, ki nas najverjetneje čakajo v prihodnosti in vprašanjem ali smo nanje resnično pripravljeni.

Ključne besede — kritična infrastruktura, neprekinjeno poslovanje, elektronske komunikacije, izjemna stanja

Abstract — This Article is an attempt to identify critical infrastructure that is vital for electronic communication services to be fully functional. It doesn't have ambition to define neither the services nor the infrastructure, failure of which would endanger vital state functions. The answer to the last question will give the user itself-the State, when it defines network critical parts and elements, and therefore come to a decision in what range and in what way to protect them. Further on in this Article there is a short introduction into the legislation about critical infrastructure. At the end we identify some of the forthcoming challenges and question whether we are really ready to cope with them.

Keywords — critical infrastructure, business continuity management, electronic communications

I. UVOD

Pri identifikaciji kritične infrastrukture državnega pomena na področju elektronskih komunikacij se je smiselno vprašati, katere storitve so ključnega pomena za delovanje države? Katere storitve elektronskih komunikacij na primer podpirajo funkcionalnost energetske in prometne kritične infrastrukture? Ugotovimo, da skoraj ni storitve, brez katere bi lahko omenjena sektorja nemoteno delovala. Storitve elektronskih komunikacij so tako pomembne podporne funkcije, da njihovo nedelovanje ali omejena/pomanjkljiva funkcionalnost resno vpliva tako na vsakdanje življenje posameznika, procese v gospodarstvu, na nacionalno varnost, posledično pa na samo delovanje države in njen ugled v svetu.

Na tem mestu je potrebno izpostaviti problem visokih stroškov, ki jih povzroči zagotavljanje sistema upravljanja neprekinjenega poslovanja, torej zagotavljanje celovitosti omrežja. To breme danes v večji meri nosijo zlasti operaterji elektronskih komunikacij. Zaradi tega je izredno pomembno, da vsi vpleteni deležniki pristopijo k procesu identifikacije kritične infrastrukture z vidika prepoznavanja ključnih storitev pravično, odgovorno in sistematično.

II. ZAKONODAJNI OKVIR

Direktiva Sveta Evropske unije o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite [1] v svojem 12. členu narekuje državam članicam izvajanje direktive oziroma sprejetje predpisov, potrebnih za uskladitev z njenimi določili, osredotočena pa je na energetski in prometni sektor.

Za izvedbo navedene zahteve je bila na Ministrstvu za obrambo, ki je bilo odgovorno za implementacijo, ob usmerjanju Medresorske koordinacijske skupine za usklajevanje priprav za zaščito kritične infrastrukture [2] pripravljena Uredba o evropski kritični infrastrukturi [3].

V začetku leta 2014 so bile sprejete Spremembe in dopolnitve osnovnih in sektorskih kriterijev kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji [4], ki spreminjajo/dopolnjujejo Sklep Vlade RS št. 80200-1/2012/5, z dne 17. 10. 2012.

III. OSNOVNI IN SEKTORSKI KRITERIJI KRITIČNOSTI

Na podlagi definicije osnovnih ter sektorskih kriterijev za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji so ministrstva in Banka Slovenije ob usklajevanju v Medresorski koordinacijski skupini za usklajevanje priprav za zaščito kritične infrastrukture v Republiki Sloveniji predlagali in utemeljili konkretno kritično infrastrukturo Republike Slovenije po sektorjih kritične infrastrukture, ki je bila predložena Vladi Republike Slovenije v obravnavo in potrditev. Vlada je s sklepom naložila nosilcem kritične infrastrukture državnega pomena oblikovanje ukrepov za njeno zaščito, Medresorski koordinacijski skupini za usklajevanje priprav za zaščito kritične infrastrukture v Republiki Sloveniji pa pripravo predloga normativno-pravnega akta, ki bo urejal kritično infrastrukturo Republike Slovenije.

Vlada Republike Slovenije je s sklepom, št. 80200-2/2014/8, z dne 10. aprila 2014, določila kritično infrastrukturo državnega pomena v Republiki Sloveniji.

Dne 11.7.2014 so bili določeni veljavni kriteriji kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji [5], ki izhajajo iz definicije kritične infrastrukture državnega pomena v Republiki Sloveniji, ki jo je na predlog Medresorske koordinacijske skupine za usklajevanje priprav za zaščito kritične infrastrukture v Republiki Sloveniji potrdila Vlada Republike Slovenije dne 19. 4. 2010. Vlada Republike Slovenije je naložila ministrstvom in vladnim službam, da pri pripravi predpisov, izvajanju priprav in drugih aktivnosti za zaščito kritične infrastrukture upoštevajo definicijo kritične infrastrukture državnega pomena v Republiki Sloveniji.

Sektorji kritične infrastrukture Republike Slovenije so:

- sektor kritične infrastrukture, ki zagotavlja energetsko podporo,
- sektor kritične infrastrukture, ki zagotavlja prometne povezave,
- sektor kritične infrastrukture, ki zagotavlja preskrbo s hrano,

- sektor kritične infrastrukture, ki zagotavlja preskrbo s pitno vodo,
- sektor kritične infrastrukture, ki zagotavlja zdravstveno oskrbo,
- sektor kritične infrastrukture, ki zagotavlja finance,
- sektor kritične infrastrukture, ki zagotavlja varstvo okolja,
- sektor kritične infrastrukture, ki zagotavlja informacijsko in komunikacijsko podporo.

Ker so pristojnosti Agencije za komunikacijska omrežja in storitve (v nadaljevanju: Agencija) omejene na področje elektronskih komunikacij, se v nadaljevanju osredotočamo na sektor kritične infrastrukture, ki zagotavlja informacijsko in komunikacijsko podporo.

IV. KRITIČNA INFRASTRUKTURA ZA ZAGOTAVLJANJE INFORMACIJSKE IN KOMUNIKACIJSKE PODPORE

Skladno z dokumentom Ministrstva za obrambo »Veljavni kriteriji kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji« [5] so…začnimo z osnovnimi kriteriji za določitev kritične infrastrukture Republike Slovenije:

- nedelovanje, ki povzroči ali vpliva na smrt večjega števila od 50 oseb,
- nedelovanje, ki povzroči pomemben vpliv na zdravje prebivalstva v takšni meri, da je potrebno hospitalizirati več kot 100 oseb za več kot teden dni,
- nedelovanje, ki povzroči poškodovanje, uničenje dejavnosti, objektov ali območij z vplivom na nacionalno varnost Republike Slovenije do te mere, da je oteženo izvajanje obrambe, notranje varnosti ali varstva pred naravnimi in drugimi nesrečami,
- nedelovanje, ki vpliva na izvajanje gospodarske ali druge dejavnosti v obsegu povzročene škode ali izpada dohodka več 10 mio evrov na dan,
- nedelovanje, ki vpliva na prekinitev preskrbe s pitno vodo ali hrano za več kot teden dni, za prebivalstvo v obsegu preko 100.000 ljudi,
- nedelovanje, ki vpliva na prekinitev preskrbe z električno energijo za 3 dni ali z zemeljskim plinom za več kot teden dni za prebivalstvo v obsegu preko 100.000 ljudi,
- nedelovanje, ki vpliva na izpad oskrbe z naftnimi derivati za več kot teden dni, za prebivalstvo na območju preko 100.000 ljudi,
- nedelovanje, ki vpliva na veliko škodo na kopenski ali vodni življenjski prostor na površini več kot 100 ha,
- nedelovanje, ki povzroči informacijski ali komunikacijski izpad podpore delovanja drugih kritičnih infrastruktur do 24 ur,
- nedelovanje, ki povzroči čezmejne posledice v drugih državah glede na predhodne kriterije.

V 3. točki prej omenjenega dokumenta [5] so poleg definicije in osnovnih kriterijev za določanje kritične infrastrukture ob upoštevanju specifik posameznega sektorja, navedeni še sektorski kriteriji. Za sektor, ki zagotavlja informacijsko in komunikacijsko podporo je kriterij kritičnosti določen s trajanjem nedelovanja storitev. Ko se z analizo ugotovi, da nedelovanje elektronsko komunikacijske opreme, omrežja ali storitve, ki podpirajo ključne funkcije v državi in ki se nanašajo na zagotavljanje oziroma delovanje enega od sektorjev kritične infrastrukture, povzroči izpad podpore za več kot 6 oziroma 24 ur, je potrebno sprejeti vse potrebne ukrepe, ki bi to pomanjkljivost odpravili. Na podlagi tega kriterija je možno določiti obseg in elemente kritične infrastrukture elektronskih komunikacij.

V 4. točki istega dokumenta [5] je kritična infrastruktura razvrščena še po prioritetah delovanja, oziroma neposrednem vplivu na delovanje drugih sektorjev se pravi z upoštevanjem prioritet kritičnosti: zagotavljanje električne energije, informacijsko komunikacijska podpora, preskrba s pitno vodo, preskrba s hrano, zagotavljanje zdravstvene oskrbe, preskrba z naftnimi derivati, zagotavljanje železniškega prometa, zagotavljanje letalskega prometa, delovanje pristaniške dejavnosti, preskrba s plinom, delovanje plačilnega, prometa, zagotavljanje oskrbe z gotovino, delovanje državnega proračuna in varovanje zdravega okolja.

Informacijsko komunikacijska podpora se na tem seznamu pojavi na drugem mestu, takoj za zagotavljanjem električne energije. Da je zagotavljanje električne energije prva prioriteta kritičnosti je samoumevno, saj je tako kot delovanje ostalih sektorjev tudi delovanje elektronskih komunikacij močno odvisno od razpoložljivosti električne energije.

Glede na slednje dejstvo, torej, da je informacijsko komunikacijska podpora po svoji pomembnosti uvrščena tako visoko, pa se zdi skoraj neverjetno, da zakon, ki ureja elektronske komunikacije [7], torej zakon, ki operaterjem, ki zagotavljajo elektronska komunikacijska omrežja in storitve nalaga obveznosti v zvezi z njihovim zagotavljanjem, ne pozna pojma »kritična infrastruktura«. Res je, da je ta določena v drugih predpisih, ki so bili uvodoma predstavljeni tudi v tem prispevku. Regulator pa se sprašuje, kako je z nadziranjem izvajanja teh predpisov. V uvodnem delu je bilo že rečeno, da je Vlada Republike Slovenije naložila ministrstvom in vladnim službam, da pri pripravi predpisov, izvajanju priprav in drugih aktivnosti za zaščito kritične infrastrukture upoštevajo definicijo kritične infrastrukture državnega pomena v Republiki Sloveniji. Glede na to, da v ZEKom-1 aktivnosti za zaščito kritične infrastrukture niso eksplicitno urejene, se sprašujemo, kateri predpis kritično infrastrukturo ureja in kateri organ nadzoruje aktivnosti zagotavljanja nemotenega delovanja kritične infrastrukture?

Zakon o elektronskih komunikacijah [7] v prvem odstavku 83. člena operaterjem nalaga, da morajo v primeru izjemnih stanj zagotavljati nemoteno delovanje tistih delov omrežja, ki so nujni za nemoteno delovanje omrežij nosilcev varnostnega in obrambnega sistema ter sistema zaščite in reševanja. Za čim krajše izpade teh omrežij morajo operaterji po potrebi predvideti tudi nadomestne poti. S tem namenom morajo svoje ukrepe predhodno uskladiti z nosilci varnostnega in obrambnega sistema zaščite in reševanja.

V. IZJEMNA STANJA IN VLOGA REGULATORJA

Izjemna stanja za potrebe zakona o elektronskih komunikacijah [7] so vojno ali izredno stanje, stanje nastalo zaradi naravnih ali drugih nesreč ter katastrofalni izpad omrežja.

Agencija kot nadzornik nad izvajanjem 84. člena omenjenega zakona, ki ureja razpoložljivost javno dostopnih storitev preverja, ali izvajalci javno dostopnih telefonskih storitev sprejmejo ustrezne tehnične in organizacijske ukrepe,

ki omogočajo, da so njihove dejavnosti v primeru izjemnih stanj čim manj motene. Z ukrepi, ki jih sprejmejo, morajo zagotoviti razpoložljivost javno dostopnih telefonskih storitev v najkrajšem času in zlasti **neprekinjen** dostop do in uporabo številke za klice v sili 112, številke policije 113 in enotne evropske številke za prijavo pogrešanih otrok 116 000. Navedena zakonska določba je spodbudila Agencijo k pogovoru z operaterji in analizi njihovih izkušenj pri spopadu s posledicami žleda v februarju 2014. Agencija je dala pobudo za bolj formalizirano neformalno povezovanje operaterjev mobilnih javnih komunikacijskih storitev v primeru naravnih nesreč večjih razsežnosti. K povezovanju smo pritegnili tudi Upravo RS za zaščito in reševanje (URSZR), še posebno zaradi dejstva, da je bilo v konkretnem primeru močno prizadeto tudi delovanje storitve klica v sili na 112. Pod okriljem URSZR je sedaj v nastajanju Načrt za sodelovanje operaterjev pri zagotavljanju delovanja TK storitev (sploh storitve klica v sili - 112) v primeru izjemnih stanj. Osnovni cilj je poiskati skupne rešitve glede učinkovitih mehanizmov medsebojne pomoči (državne in medoperaterske) pri vnovičnem čim hitrejšem vzpostavljanju storitve za klic v sili v primeru izpada zaradi izjemnih stanj. Z ustrezno koordinacijo in souporabo zmogljivosti vseh deležnikov se lahko bistveno optimizira proces vzpostavljanja in samo delovanje storitev v izjemnih stanjih. Več o tem bo v nadaljevanju povedal predstavnik URSZR. Takšne oblike sodelovanja države in industrije imajo tudi mednarodno primerjalno najboljše učinke, veliko boljše kot enostransko določanje (npr. s strani države) obveznosti deležnikom. Zgolj in samo nalaganje obveznosti, ki za sabo potegnejo med ostalim tudi precejšnja finančna bremena, na ramena industrije, ne bodo prinesla tako učinkovitih rezultatov. Največji izziv pri organiziranju takšnih oblik sodelovanja pa je na pravi način spodbuditi deležnike, da prepoznajo svojo družbeno odgovornost in vse prednosti - tudi lasten interes za tovrstno sodelovanje.

Neprekinjen dostop do številk za klic v sili (112, 113 in 116 000) je zahteva ZEKom-1, ki je v primeru nesreč večjih razsežnosti praktično neizvedljiva. Po več kot 2 leti veljavni določbi operaterji še vedno ne vedo, kateri so deli njihovega omrežja, ki so nujni za delovanje omrežij nosilcev varnostnega in obrambnega sistema ter sistema zaščite in reševanja, za katere veljajo posebne zahteve glede redundance. Agencija kot nadzornik izvajanja te določbe pa še vedno nima jasnih odgovorov o predmetu nadzora. S tem nakazujemo le nekaj težav pri izvajanju zakona, zakonodajalec pa bo presodil ali so potrebne spremembe.

VI. GROŽNJE IN RANLJIVOSTI

Nekaj primerov ogroženosti in ranljivosti infrastrukture zaradi naravnih nesreč smo izpostavili, večina slušateljev pa je to tudi doživela, ko je Slovenijo prizadel lanskoletni žled. Zato se bomo v nadaljevanju bolj posvetili kibernetičnim tveganjem, ki bodo v prihodnosti zagotovo vse bolj aktualna. Optimistični pogled na kibernetična tveganja je prepričanje, da je najhujše, kar se nam lahko zgodi nedelovanje fiksnih in mobilnih javnih komunikacij ter interneta. Dejstvo je, da bi bila brez delujočega interneta marsikatera storitev otežena, vseeno pa nedelovanje ne bi povzročilo katastrofičnih posledic. Optimistično pa bi bilo tudi prepričanje, da je kritična infrastruktura, ki ni del interneta, npr. storitev klica v sili, tako robustna in zavarovana, da je imuna na kibernetične napade [6]. Drži, da je kritična infrastruktura bolje zavarovana in da jo je težje ogroziti, vendar je tehnično gledano na enak način ranljiva. V preteklosti, ko so bila telekomunikacijska omrežja ločena po storitvah in med seboj šibko povezana, so bila tudi tveganja za zlorabo omrežij bistveno manjša. Zlorabe so se izvajale večinoma v obliki nepooblaščenih fizičnih dostopov. Danes govorimo o konvergentnih omrežjih in kibernetičnem prostoru, kjer je oddaljeni dostop do omrežja nekaj povsem običajnega. Računalniški zanesenjaki, ki vdirajo in nepooblaščeno dostopajo v računalniška omrežja, imenujmo jih hekerji, se dobro znajdejo v kibernetičnem prostoru. Za njih ni nemogočega. Bolj je omrežje zavarovano, večji je zanje izziv. To počnejo zaradi zaslužka, aktivizma, samo dokazovanja, pridobivanja informacij itd.

Hekerje je na splošno možno razdeliti v tri skupine: hekerske aktiviste, kibernetične teroriste in kibernetične kriminalce. Vse tri skupine uporabljajo enaka orodja in tehnike, le da z vidika ogrožanja kritične infrastrukture, kibernetični kriminalci niso problematični. Njihov motiv je zaslužek in njihov primarni cilj ni povzročanje škode z vidika celovitost ali funkcionalnosti omrežja. Vsekakor pa je pri analizi tveganja potrebno upoštevati tudi njihovo delovanje. Z vidika ogrožanja kritične infrastrukture so veliko bolj problematični hekerji aktivisti in kibernetični teroristi. Posebna kategorija so kibernetični vojaki [8], ki jih urijo države za doseganje svojih političnih ali gospodarskih ciljev. Vendar, teh v prispevku ne bomo obravnavali.

Hekerski aktivisti so dobro organizirani, se združujejo, izmenjujejo informacije in imajo skupne cilje za napad. So nekakšna vrsta kibernetičnih uporniških gibanj, ki protestirajo zoper globalizacijo, onesnaževanje okolja, borzo, genetsko spremenjeno hrano itd. Svoje hekerske napade usmerjajo na mednarodne organizacije, kot so mednarodna borza, svetovna banka, G8 itd. S svojim delovanjem lahko povzročijo znatno gmotno škodo, vendar z vidika varovanja kritične infrastrukture niso tako problematični kot kibernetični teroristi. Hekerski aktivisti delujejo bolj ali manj odkrito, celo napovejo napade, so bolj predvidljivi in posledično manj nevarni. Njihova najbolj vidna in prepoznavna aktivnost je, na primer, izdelava lažne spletne strani, ki je skoraj enaka originalni in propagira njihove cilje. Drug značilni primer njihove aktivnosti je sprememba vsebine tuje spletne strani za lastno korist, za promocijo svojih aktivnosti, preusmerjanje prometa ipd.

Ko gre hekerski aktivist v ilegalo, se prelevi v kibernetičnega terorista. O kibernetičnih teroristih ne vemo veliko, ker delujejo v ilegali. O njih se več izve na podlagi njihovega delovanja. FBI pravi, da je kibernetični terorizem politično motivirani napad na informacije, računalniške sisteme, računalniške programe in podatke, z namenom izvajanje nasilja nad nevojaškimi cilji s strani podtalnih skupin ali tajnih agentov [6]. Njihov priljubljeni cilj napada je infrastruktura tujih držav. S svojim delovanjem ustvarjajo negotovost in paniko med civilnim prebivalstvom, nezaupanje v vlado, vplivajo na ekonomsko stabilnost države itd. Zaradi tega je delovanje kibernetičnih teroristov resna grožnja za varnost kritične infrastrukture in jih je pri analizi tveganja potrebno upoštevati.

VII. ZAKLJUČEK

Identifikacija kritične infrastrukture na področju elektronskih komunikacij ne bo enostavna naloga. Še manj pa določanje in implementacija ukrepov za zavarovanje le-te.

Postavlja se vprašanje iskanja optimalnega razmerja med stroški in zahtevami; in ne nazadnje, če in v kolikšnem obsegu naj to breme prevzamejo operaterji.

LITERATURA

[1] Direktiva Sveta Evropske unije o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite, Ur. l. EU št. 114/2008

[2] http://www.mo.gov.si/si/delovna_podrocja/zascita_kriticne_infrastrukture/medresorska_koordinacijska_skupina_za_usklajevanje_priprav_za_zascito_kriticne_infrastrukture/

[3] Uredba o evropski kritični infrastrukturi, objavljena (Ur. l. RS št. 35/2011)

[4] Spremembe in dopolnitve osnovnih in sektorskih kriterijev kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji, sklep Vlade RS št. 80200-2/2013/3, z dne 9. 1. 2014

[5] http://www.mo.gov.si/si/delovna_podrocja/zascita_kriticne_infrastrukture/

[6] Stefano Baldi, Eduardo Gelbstain, Jovan Kurbalija: Hactivism, Cyber-terorism and Cyberwar, Diplo 2003

[7] Zakon o elektronskih komunikacijah (Ur. l. RS št. 109/2012)

[8] http://www.washingtonexaminer.com/pentagon-struggles-to-embrace-cyber-warriors/article/2561514

Katja Kmet že več kot desetletje deluje na področju elektronskih komunikacij. Kot pravna strokovnjakinja je na Agenciji za komunikacijska omrežja in storitve svojo poklicno pot začela na področju reševanja uporabniških in medoperaterskih sporov, nadaljevala kot pooblaščena oseba agencije v Sektorju za nadzor, ki ga sedaj tudi vodi. Aktivno sodeluje v evropskih delovnih skupinah na področju varnosti (ENISA) in nevtralnosti interneta pri evropskem združenju regulatorjev BEREC.

Mag. **Albin Poljanec** je diplomiral leta 1984 na Fakulteti za elektrotehniko na Univerzi v Beogradu, s področja telekomunikacij. Leta 1996 je magistriral na Fakulteti za organizacijske vede na Univerzi v Mariboru, s področja managementa kakovosti. Zaposlen je kot specialist za nadzor telekomunikacij na Agenciji za komunikacijska omrežja in storitve.

Organization of the communication system and information support during floods in Slavonia in 2014

Davor Spevec, National Protection and Rescue Directorate, Zagreb, Croatia

Abstract — The paper gives a short description of the way the communication systems and information support was organized during protection, rescue and flood recovery activities in Slavonia during May and June 2014.

Keywords — flood, radio communications, telecommunications, information support

Povzetek — Ta članek opisuje, kako so bili organizirani komunikacijski sistemi in kakšna je bila informacijska podpora pri aktivnostih zaščite in reševanja med poplavami, ki so prizadele Slavonijo maja in junija 2014.

Ključne besede — poplava, radijske komunikacije, telekomunikacije, informacijska podpora

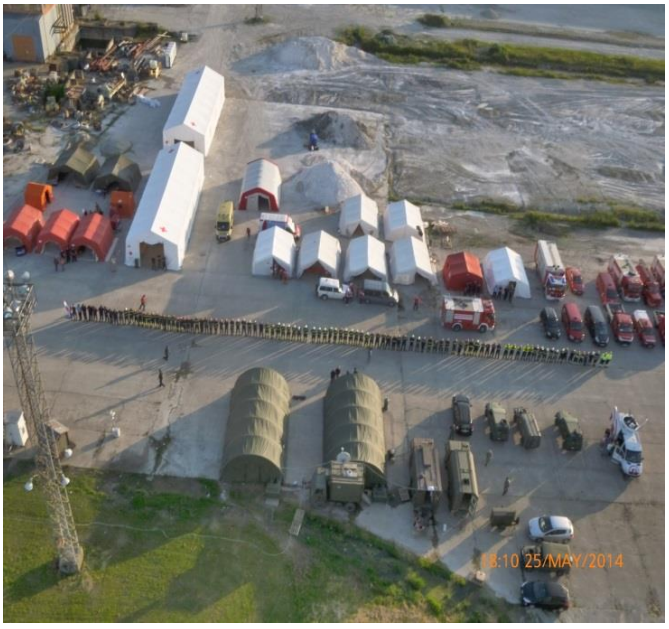
I. INTRODUCTION

Last year, 2014, will be remembered in the Republic of Croatia as the year of weather extremes and substantial damages (over €600 M) caused by severe weather conditions, from freezing rain that brought Gorski kotar area to a standstill, floods in the area of central Croatia in February, floods in the area of Posavina and Slavonia in May to floods in the area of western Slavonia in September. This paper will focus on the organization of communication systems and information support which was organized as support to the headquarters and operational forces for the area of Županjska Posavina after the embankment broke on 17 May.

Heavy rainfall during May 2014, particularly in the week of 12th to 17th of May, in the area of the Republic of Croatia, primarily Slavonija and Baranja and Bosnia and Herzegovina and Serbia, caused the rise in water levels of the Sava river tributaries, both left and particularly right tributaries: Una, Bosna and Vrbas. In some areas, there was a record-breaking amount of rainfall, and in many places the amount of rainfall in these few days exceeded monthly maximums for the entire month of May. Consequently, water levels rose downstream from Jasenovac to Županja. At the same time, there were maximum water levels of the river Sava from Slavonski Kobaš to Županja, and of the rivers Bosna, Vrbas and Drina since records began. Besides a sudden and very heavy rainfall in the first half of May, the fact that the soil had already been saturated from the extreme rainfall in April additionally worsened the situation.1

Consequently, in the afternoon hours of 17 May 2014, the embankment broke in the area of Rajevo Selo and Račinovci, and Sava waters overflowed in the low-lying hinterland of Županjska Posavina. Seven villages were flooded, there were two casualties, 8,900 inhabitants and over 9,000 heads of livestock were evacuated, 7,500 objects were damaged.

Croatian Firefighting units and Croatian Armed Forces joined the domicile population in flood defense activities. On 20 May 2014, after the terrain analysis and after establishing that the resulting consequences were too overwhelming for the local and regional self-government, Croatian government declared a state of emergency for the area of Vukovar-Srijem County. On the same day, extraordinary session of the National Protection and Rescue Headquarters was held in Zagreb, during which it was decided that "Sladorana" Ltd. in Županja will be the location of the relocated command and communications center (camp) of the protection and rescue operations forces tasked with managing activities of operational forces and protection and rescue forces in-field – Picture 1.



Picture 1: Camp in Županja

The camp served as a location for operational capacities and experts from the National Protection and Rescue Directorate (NPRD), Ministry of Agriculture and Hrvatske vode (Croatian Water), Ministry of Interior (MoI), Croatian Armed Forces, crisis headquarters of the Ministry of Health, Ministry of Foreign and European Affairs, Ministry of Environmental and Nature Protection, Ministry of Construction and Physical Planning, Croatian Mountain Rescue Service, Croatian Red Cross and Croatian Mine

[1] From the report by the Ministry of Agriculture.

Action Centre. Around a hundred people permanently resided in the camp, and the volunteer camp was set up nearby. Operational forces were located in the vicinity of the flooded area.

The State Information and Communication Protection and Rescue Sector, as a sector within the NPRD, was tasked with providing the communication system for coordination and information support for the needs of the HQ and operational forces. For this reason, the staff of IT Department and Communication Technology Department was deployed to Županja, and relocated section of the National Protection and Rescue Information and Communication System was established there.

II. COMMUNICATIONS

A. Radio communications

Upon arrival in the field it was established that the communication infrastructure was insufficient for the activities that needed to be carried out. As this is the low-lying area, the entire electrical network, together with the mobile operator equipment, was flooded, resulting in the loss of GSM signal. The only option available was to use the Bosnia and Herzegovina mobile operators' signal, resulting in high costs. The flooded area was not even covered by the NPRD radio network, primarily used by firefighters, Croatian Mountain Rescue Service and Red Cross.

i. Tetra

Plan	Red.br	Dužnost	Organizacija	Mjesto	ID broj	Pozivna oznaka
d01-ISKRA	1	Ravnatelj	DUZS	Zagreb	600101	**DINARA 100**
	2	Državni centar	DIKS	Zagreb	600000	**DINARA**
	2	Državni centar Županja	DIKS	Županja	600001	**DCŽUPANJA 1**
	3	Zamjenik ravnatelja	DUZS	Zagreb	600103	**DINARA 102**
	4	Glavni vatrogasni zapovj	SV	Zagreb	300101	**ISKRA 100**
	5	PomGVZ za kopno	SV	Zagreb	300104	**ISKRA 200**
	6	Načelnik	DIKS	Zagreb	600102	**DINARA 200**
	7	Načelnik	DCZiS	Zagreb	600113	**DINARA 201**
	8	Glavni zapovjednik CZ	SCZ	Zagreb	700101	**CETINA 100**
	9	Pročelnik	PUZS	Vukovar		**VUKOVAR 100**
	10	Pročelnik	PUZS	Rijeka	625101	**RIJEKA 100**
	11	Koordinator	HGSS	Županja	673121	**GSS**
	12	Koordinator	MUP	Županja	683121	**MUP**
	13	Koordinator	MinZdravlja	Županja		**HITNA**
	14	Koordinator	HCK	Županja	300108	**CRVENI KRIŽ**
	15	Župan	Županija	Županja		**ŽUPANIJA 1**
	16	Dožupan	Županija	Županja	300109	**ŽUPANIJA 2**
	17	Koordinator	MinPoljop	Županja	300116	**VETERINA**
	18	Zapovjedništvo	HV	Županja		**ORAO**
	19	Zapovjednik	DIP	Rijeka	665122	**RIJEKA**
	20	Izdvojeno zapovjedništv	SV	Drenovci	107531	**DRENOVCI 100**
	21	ZamPomGVZ	SV	Koprivnica	300105	**ISKRA 201**
	22	Pilat	DIKZiS	Zagreb	600111	**Radio 100**
	23	Zapovjednik	DIP	Rijeka	665121	**Rijeka 201**
	24	Vođa ekipe	DIP	Rijeka	340122	**Rijeka 202**
	25	Škalamera	PUZS	Rijeka		**Rijeka 100**
	26	Habijan	SV	Koprivnica	300111	**ISKRA 202**
	27	Banjan	SV	Osijek	300110	**ISKRA 203**

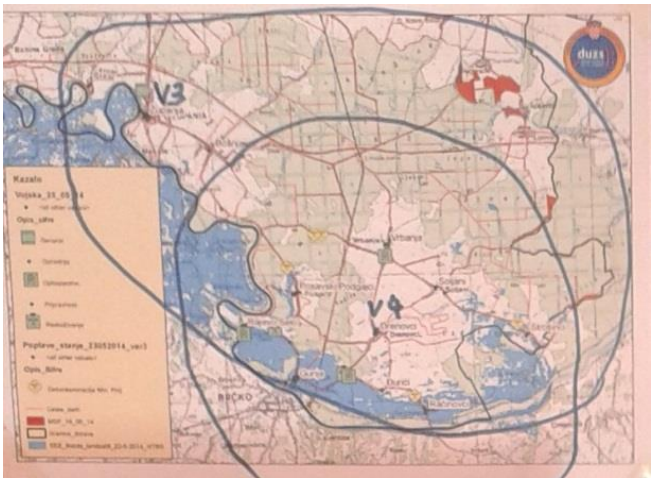
Picture 2: An example of the Tetra Work plan

The only system that remained operational was the MUPNet TETRA network, primarily used by the Ministry of Interior and also by the National Protection and Rescue Directorate. The problem was that we only had twenty TETRA radio devices at our disposal that we distributed to HQ members and operational forces coordinators. Two communication groups were used in the field, one for HQ needs and the other one for coordinating forces in the field.

The State Protection and Rescue Center (DC ZiS) used two stationary TETRA stations to check connectivity with the users every morning at 8 o'clock, according to the Work plan. An example of the Tetra Work plan can be seen in Picture 2. The Work plan was updated daily considering users in the field. The users of TETRA radio stations used the same during protection and rescue activities by using their own codes.

ii. Analog radio network

The NPRD's analog radio network was used for the activities of operational protection and rescue forces that were directly involved in flood recovery. Two repeaters were set up to ensure better coverage, one on the silos in Županja (V3) for coordination in the Županja area and the second one in Drenovci (V4) on the HT antenna mast the coverage of the flooded area. The approximate coverage plan is shown in Picture 3.



Picture 3: The area of V3 (Županja) coverage and V4 (Drenovci) coverage

Repetitor	Red.br	NAZIV	Pozivna oznaka
V3	1	Zdenko Lovrić	DUZS
	2	Babina greda	Babina greda 1
	3	Gunja	Gunja 1
	4	Gunja	Gunja 2
	5	Štitar	Štitar 1
	6	Štitar	Štitar 2
	7	Županja	Županja 1
	8	Županja	Županja 2
	9	Bošnjaci	Bošnjaci 1
	10	Bošnjaci	Bošnjaci 2
	11	Drenovci	Drenovci 1
	12	Drenovci	Drenovci 2
	13	Vrbanja	Vrbanja 1
	14	Vrbanja	Vrbanja 2
	15	Županijski stožer	Županijski stožer

Picture 4: Work plan in the analog network

The activity of V3 repeater was very weak, while the activity of V4 repeater located in Drenovci was at a very high level. The State Information and Communication Protection and Rescue Sector provided 40 portable radio stations to be used in the protection and rescue analog radio network and distributed them according to needs expressed by firefighting and civil protection coordinators. The users of the analog

network were primarily operational protection and rescue forces and authorized members of local self-government in the flood-affected area. An example of Work plan in the analog network is shown in Picture 4.

In the tent on Sladorana location in Županja, a portable set owned by NPRD and designed for these purposes was used for work in the analog network (V3, V4 and 8th channel). It is shown in Picture 5. The portable set allows speech and data transmissions through the analog radio communication shortwave system of the NPRD, which was not in use this time.

Picture 5: Portable radio communications set

The activity on the 8th channel was conducted on a simplex channel for the needs of organizing camp to accommodate volunteers in Županja.

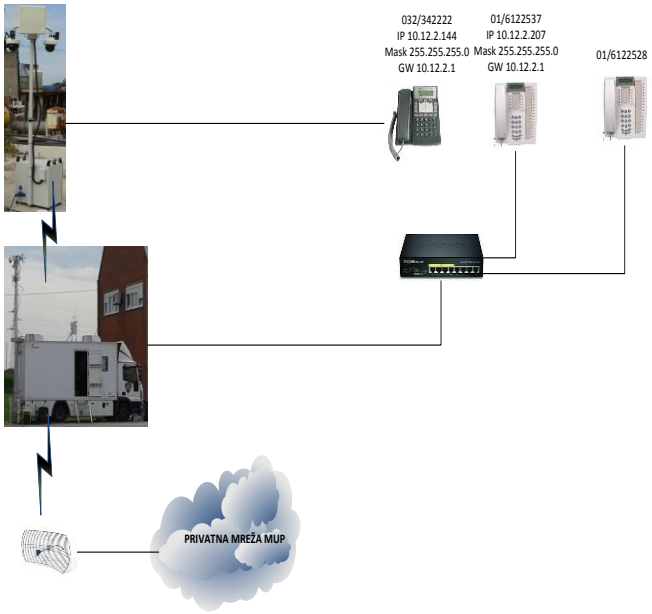
B. *Telecommunications*

i. *Fixed telephony*

Voice communication in the public communication network was secured through the Ministry of Interior's Communications network, as shown in Picture 6, and supported solely through IP technology.

Access to the Ministry of Interior's Communications network was provided via wireless connection through the location on the silos where the MoI has access point to the central location and also on the other side, Sladorana, where the command vehicle was located.

For the purpose of providing the redundant route between the tent and the command vehicle, wired connection was provided using Cat5e UTP cable with PoE that supported two H.323 phones. Both phones were connected through the MoI's network to the gatekeeper of the telephone exchange located in Zagreb. For this reason, both phones had Zagreb dial code. The other direction was provided through combining wireless and wired connection via container with cameras. This phone was connected to the gatekeeper of the telephone exchange in Vinkovci. This provided us with the alternative route in case of malfunction or disrupted connections.



Picture 6: Scheme of connecting telephonies through MoI's network

ii. *Mobile telephony*

For this activity, 17 mobile phones were provided that were used to coordinate operational protection and rescue forces and to organize the work of the camp. The positive thing was the fact that the service providers, HT and VIPnet provided free internet and wi-fi zones. HT also set up 4G network in Županja, enabling us to use mobile devices as redundant routing in case of need.

III. INFORMATION SUPPORT

Parallel to setting up communication infrastructure, providing IT equipment to the dislocated State Information and Communication Protection and Rescue Sector (DC ZiS) and other participants was also under way.

Our hosts in Sladorana enabled us to use electric power by extending electric cable from their object to our junction box and further on to the users. Fortunately, we didn't have to use the generator that we had brought in. They have also enabled us to use the internet, which was connected to the DC ZiS communication tent via UTP cables.

In the communication tent, besides radio equipment, two computers were installed for the DC ZiS operators, one computer for the GIS analyst, multifunctional device and color printer. Three laptops were installed in the Civil Protection command tent, and two laptops in the press tent. In the main tent, used for HQ sessions and coordination meetings, two screens and two projectors with laptops were set up.

As the internet access, besides Sladorana network, was obtained through MoI's communication vehicle, we provided internet access for all users in the camp (FREE Wi-Fi). Subsequently, the link was divided in two routers, with two kinds of internet access. One router was encrypted for the NPRD users, Croatian Fire Fighting Association and Croatian

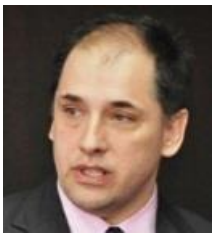
Red cross, while the other one remained open for everyone else.

During our deployment from 21 May to 14 June 2014, with a very limited number of people, we managed to:

- coordinate operational communication of the state administration bodies, emergency services, legal and physical entities;
- provide operational-communication support to protection and rescue HQ (1966 emails received i 844 emails sent);
- write and distribute situation reports to all participants, which included special reports on flood affected areas (the total of 77 situation reports written and distributed);
- participate in writing official letters related to floods (to the Ministry of Defense, Ministry of Economy, Directorate for Commodity Reserves, Ministry of Security of Bosnia and Herzegovina – the total of 52 official letters were written);
- collect and distribute hydrological, meteorological, epidemiological data and environmental pollution data from competent services and bodies, and monitor and update the data;
- exchange information and data with other countries and international organizations;
- participate in the realization of simplified border crossing procedures (the total of 101 border crossings with simplified procedures, involving 1.124 persons, 483 vehicles and 81 trailer).

IV. CONCLUSION

Having in mind the intensity of the event, the size of the affected area, the problems we encountered in the field and the limited human and material resources available, we can be very satisfied with what we accomplished. Many things would certainly have been solved more easily had it not been for the complete failure of the mobile telephony, which initially presented the biggest problem. Similarly, if we had had a larger number of TETRA devices at our disposal, we wouldn't have had to set up analog repeaters and maintain the communication system of that kind. Standard IT equipment that we used is not adequate for field conditions due to high temperatures, dust and humidity. However, the biggest drawback was the insufficient communication and information exchange among different services in the field. Technical problems, listed in the first part of the conclusion section, were solved mostly through acquiring a communication vehicle, where the entire communication and IT equipment for activities in Slavonia was placed. We also acquired a large number of radio devices and portable repeaters – analog and DMR. We are currently testing the TETRA portable repeater. The problem of insufficient communication and information exchange among services still needs to be worked on, hopefully through exercises and not real events.



Davor Spevec graduated from the Faculty of Political Sciences in Zagreb, Croatia. At the beginning of 1993, he was mobilized in the Ministry of Defense and in 1993 he became Head of the City Center for Information Samobor. In 2005, when the National Protection and Rescue Directorate was established, he became Head of 112 Centre. Since 2012 he has been Head of the State Information and Communication Protection and Rescue Sector.

Pomen usklajenega ukrepanja ponudnikov IKT ob velikih naravnih in drugih nesrečah

Boštjan Tavčar, Uprava RS za zaščito in reševanje, Ljubljana

Povzetek — Članek opisuje pomen usklajenega ukrepanja ponudnikov IKT ob velikih naravnih in drugih nesrečah. Sodelovanje med operaterji in pomoč države so ključni za čim hitrejšo ponovno vzpostavitev IKT storitev. Kako se ob tem izogniti pastem modernih tehnologij, ki so praviloma bolj ranljive od klasičnih, je velik izziv. Ali je to mogoče doseči z večjo liberalizacijo upajoč, da bo konkurenca na trgu prisilila operaterje, da nam bodo ponujali storitve ustrezne kakovosti, ali z večjo regulacijo in nadzorom države? Trezen in argumentiran razmislek je več kot nujen. Ali se tega že zavedamo, je drugo vprašanje.

Ključne besede — 112, klic v sili, kritična infrastruktura

Abstract — Article describes the importance of a coordinated action of ICT service providers in major natural and other disasters. Cooperation between operators and state assistance are key conditions for the early restoration of ICT services. How to avoid the pitfalls of modern technologies, which are generally more vulnerable than the classic, is a major challenge. Can this be done with greater liberalization hoping that competition in the market forced the operators that we will offer the services of adequate quality or greater regulation and supervision of the country? Sober reflection is more than necessary.

Keywords — 112, emergency call, critical infrastructure

I. UVOD

Ujma z žledom, ki je prizadela Slovenijo februarja leta 2014, je pokazala vso ranljivost sodobnih telekomunikacijskih sistemov. Okvare na električnih daljnovodih in omrežjih ter zelo otežen oziroma na posameznih mestih onemogočen dostop do izpostavljenih telekomunikacijskih objektov so bili glavni vzroki izpada javne mobilne telefonije na širših območjih. Če zraven prištejemo še izpade fiksnih telefonskih IP-priključkov, ki za svoje delovanje potrebujejo električno energijo, lahko z gotovostjo zatrdimo, da je v prvem obdobju trajanja ujme veliko ljudi ostalo brez telekomunikacijskih povezav in s tem brez možnosti klica v sili na 112. Obseg in teža posledic ujme sta presegala zmožnosti operaterjev za hitro ponovno vzpostavitev delovanja njihovih omrežij na najbolj prizadetih območjih. Z medsebojno pomočjo ter ob pomoči sil za zaščito, reševanje in pomoč, bi bile težave veliko hitreje odpravljene oziroma bi bilo lahko vzpostavljeno vsaj delovanje številke za klic v sili 112.

Največji problemi so bili z zagotavljanjem električne energije, saj se je pod težo žleda porušila večina nadzemnih električnih vodov. Težave so bile zaradi pomanjkanja električnih agregatov, zato smo v Štabu Civilne zaščite Republike Slovenije v sodelovanju z distributerji električne energije naredili načrt prednostne preskrbe z električno energijo. Vanj smo na pobudo Telekoma Slovenije že v ponedeljek, 3. 2. 2014, vključili 36 telekomunikacijskih objektov, od tega pet v prvo prioriteto. Na vseh telekomunikacijskih objektih v upravljanju Uprave RS za zaščito in reševanje ter Službe za informatiko in komunikacije Ministrstva za obrambo smo zagotovili napajanje iz električnih agregatov, na katere smo priključili tudi operaterje javnih telekomunikacijskih storitev. Kadar so to dopuščale slabe vremenske razmere, smo omogočali helikopterske prevoze agregatov na ključne telekomunikacijske objekte, ki niso bili dostopni oziroma je bil dostop prenevaren. Omogočali smo tudi preskrbo agregatov z gorivom.

Vlada Republike Slovenije je v svojem sklepu ugotovila, da je bilo aktiviranje in delovanje sil za zaščito, reševanje in pomoč ter javnih gospodarskih družb, med njimi Telekoma Slovenije, na vseh ravneh ukrepanja pravočasno, njihovo delovanje organizirano, prizadevno in v okviru danih možnosti učinkovito. Vlada Republike Slovenije je vsem izrekla posebno priznanje za njihovo pomoč in požrtvovalnost.

Na podlagi pridobljenih izkušenj smo se v sodelovanju z Agencijo za komunikacijska omrežja in storitve Republike Slovenije odločili, da bomo z operaterji javne mobilne telefonije pripravili načrte skupnega usklajenega ukrepanja v primeru velikih naravnih in drugih nesreč ter izjemnih stanjih v telekomunikacijskih omrežjih.

II. NAČRT SKUPNEGA USKLAJENEGA UKREPANJA

Z načrtom skupnega usklajenega ukrepanja operaterjev želimo v naprej uskladiti potrebne ukrepe, obveze in postopke za čim bolj nemoteno delovanje informacijskih in komunikacijskih sistemov v primeru velikih naravnih in drugih nesreč, še zlasti delovanje storitev za prenos klicev v sili na 112. Zakon o elektronskih komunikacijah v 84. členu določa, da morajo operaterji sprejeti ustrezne tehnične in organizacijske ukrepe, ki omogočajo, da so njihove dejavnosti v primeru izjemnih stanj čim manj motene. Z njimi morajo v najkrajšem možnem času zagotoviti razpoložljivost javno dostopnih telefonskih storitev, še zlasti neprekinjen dostop in uporabo številk za klic v sili. Vlada lahko s sklepom določi tudi druge ukrepe za zagotavljanje delovanja javnih komunikacijskih omrežij ali storitev ob naravnih in drugih nesrečah ali ob katastrofalnem izpadu omrežja.

V dosedanjih dogovorih smo se osredotočili na zagotavljanje delovanja storitev omrežij mobilne telefonije. Izmenjali smo si podatke o odgovornih osebah in postopkih medsebojnega obveščanja. O vseh večjih izpadih in motnjah v telekomunikacijskih omrežjih ter v primeru prošnje za

pomoč je potrebno obvestiti Center za obveščanje Republike Slovenije. Na podlagi primerjalne analize podatkov o baznih postajah posameznih operaterjev smo določili telekomunikacijske objekte prve prioritete, upoštevajoč območja, ki jih neposredno ali posredno pokrivajo s signalom mobilne telefonije. V prvi fazi usklajevanja smo določili bazne postaje prve prioritete, na sliki 1 označeno modro in vozliščne bazne postaje, označene rdeče.

Slika 1: Bazne postaje prve prioritete v 1. fazi usklajevanja

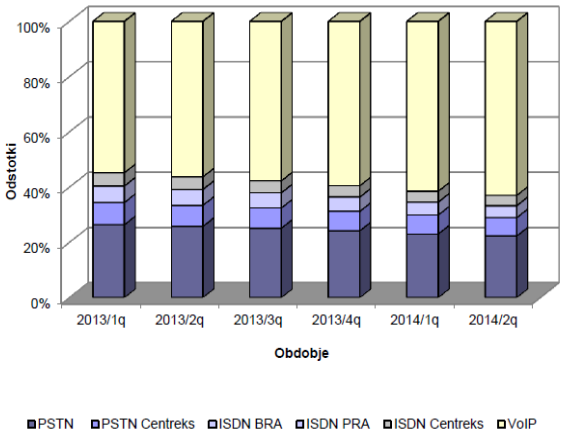
Za vse telekomunikacijske objekte bomo zbrali podatke o minimalni potrebni moči električnega priključka ter podatke o primernih mestih za namestitev in priključitev agregatov. Podatki bodo v pomoč pri prednostnem zagotavljanju preskrbe z električno energijo. V nadaljevanju moramo doseči dogovor, kdo od operaterjev bo zadolžen za prvo ukrepanje na posameznih telekomunikacijskih objektih, kjer ima opremo več operaterjev. Naredili bomo načrt pomoči države ter sil za zaščito, reševanje in pomoč v primeru, ko obseg naravne ali druge nesreče preseže zmožnost samostojnega ukrepanja operaterjev. Dogovorili se bomo o preverjanju pripravljenosti in ukrepov na vajah, ki jih organizira Civilna zaščita.

V prihodnosti bo potrebno razmisliti tudi o morebitnih spremembah in dopolnitvah zakonov ter podzakonskih aktov z namenom boljše normativne in posledično izvedbene ureditve ukrepov za zagotavljanje delovanja omrežij, še zlasti ob velikih naravnih in drugih nesrečah ter izjemnih stanjih. Zakon o elektronskih komunikacijah v sedmem poglavju sicer ureja varnost omrežij in storitev ter njihovo delovanje v izjemnih stanjih, vendar po mojem mnenju v splošnem daje premajhen poudarek razpoložljivosti in zanesljivosti. V 80. členu je zapisano, da morajo operaterji sprejeti vse potrebne ukrepe za zagotovitev celovitosti svojih omrežij, tako da se zagotovi neprekinjeno izvajanje storitev, vendar se to da razumeti predvsem v smislu varovanja pred vdori. To je mogoče sklepati tudi upoštevajoč 81. člen, ki predpisuje obvezno obveščanje nacionalnega organa za obravnavo varnostnih incidentov (SI-CERT) in Evropske agencije za varnost omrežij in informacij (ENISA). Na tem mestu se upravičeno lahko vprašamo, kako zagotoviti potrebno kakovost omrežij in storitev? Ali je to mogoče doseči z še večjo liberalizacijo upajoč, da bo konkurenca na trgu prisilila operaterje, da nam bodo ponujali storitve ustrezne kakovosti, ali z večjo regulacijo in nadzorom države. Resnica je verjetno nekje vmes.

III. TEHNOLOŠKE PASTI

Ne gre prezreti, da so telekomunikacijske storitve že davno presegle okvire podpornih storitev. Vse večja kompleksnost in ranljivost ter odvisnost ljudi od njihovih storitev jih upravičeno uvršča med kritično infrastrukturo. V 83. členu Zakona o elektronskih komunikacijah je določeno, da morajo operaterji v primeru izjemnih stanj prednostno zagotavljati delovanje tistih delov omrežja, ki so nujni za nemoteno delovanje omrežij varnostnega in obrambnega sistema ter sistema zaščite in reševanja. Svoje ukrepe morajo z državo predhodno uskladiti. Ali to pomeni, da ima država možnost vplivati na kakovost omrežij in storitev? Vprašanje je na mestu, saj operaterji lahko z uvajanjem novih tehnologij enostransko vplivajo na kakovost storitev in s tem posledično na varnost države ter posameznikov.

Z uvajanjem telefonije IP je Telekom Slovenije zmanjšal razpoložljivost govornih storitev, ki pri analognih in ISDN telefonih v najboljšem primeru znaša 99,999 % [1], na 99,80 %. Statistično gledano se je povprečni čas izpada storitev iz 0,87 sekunde na dan podaljšal na vsaj 2,9 minut dnevno. V izračunu je upoštevana najboljša možna razpoložljivost analogne in ISDN telefonije ter najboljša možna razpoložljivost telefonije IP, brez upoštevanja neprekinjenega napajanja terminalnih naprav pri naročniku. Izpad električne energije pri naročniku povzroči izpad telefonije IP, kar predstavlja še dodaten problem, še zlasti ob velikih naravnih in drugih nesrečah. Po podatkih iz Poročila o razvoju trga elektronskih komunikacij za drugo četrtletje 2014 [2] je bil delež telefonov IP v letu 2014 večji od 60 % s težnjo naraščanja.



Slika 2: Delež posameznih tehnologij fiksne telefonije, vir:AKOS

V začetku leta 2014 je Slovenijo prizadela ujma z žledom, ki je na najbolj prizadetih območjih povzročila obsežne in dolgotrajne izpade električne energije. Najbolj je bila prizadeta Notranjska. V času ujme smo v Regijskem centru za obveščanje Postojna prejeli 453 klicev na 112 iz klasičnih analognih in ISDN telefonov ter 77 klicev iz telefonov IP iz omrežja Telekoma Slovenije, ki ima 27,7 % tržnega deleža na govornem delu v telefoniji IP [2]. Sklepamo lahko, da je skoraj šestkrat več klicev iz klasičnih in ISDN telefonov posledica nedelovanja velikega števila telefonov IP zaradi izpada električne energije. Težave so bile tudi pri mobilni telefoniji, ne zgolj zaradi izpada posameznih delov omrežja temveč tudi zaradi dejstva, da imajo pametni telefoni slabo avtonomijo akumulatorskih baterij, uporabniki pa jih zaradi

izpada električne energije niso mogli napolniti. Kolikšna je torej dejanska razpoložljivost storitev mobilne in telefonije IP? Kako le-ta vpliva na varnost ljudi? Ne pričakujte odgovora, ker ne razpolagam z zadosti podatkov in si zato ne upam postavljati dokončnih zaključkov. Problematiko je v prihodnje potrebno skrbno proučiti.

Drug primer, ki bi ga rad izpostavil, je Načrt prenove državne informatike, ki med drugim predvideva prehod na državni informacijski oblak s koncentracijo strežnikov na dveh lokacijah, v Ljubljani in Mariboru. Koncentracija podatkov na zgolj dveh lokacijah bo zahtevala zmogljivo, razpoložljivo in varno komunikacijsko omrežje. Praktično vsa količina dosedanjega lokalnega računalniškega prometa v ministrstvih in drugih državnih organih se bo prenesla na zunanje telekomunikacijske povezave. V Projektu vzpostavitve državnega računalniškega oblaka – DRO [3] je predvideno, da bodo Ministrstva povezana v skupno omrežje HKOM prek namenskih in hitrih povezav MAN. Omenjena je študija, ki bo med drugim naredila primerjavo med stroški izgradnje ali nakupa obstoječih optičnih povezav in stroški najema pri komercialnih ponudnikih. Kako bodo pri primerjavi upoštevali kakovost storitev v obeh modelih, ni jasno. Zanašati se zgolj na tako imenovane sporazume SLA je nevarno, saj gre pri tovrstnih sporazumih praviloma za verigo medsebojnega zaupanja vseh deležnikov. Ali bi država s podpisom pogodbe SLA imela vpliv in kontrolo nad celotno verigo deležnikov? Odgovor je ne. Še bolj problematičen je načrt vzpostavitve privatnega oblaka, na katerega bi preselili informacijske sisteme občin in bodočih regij. Kako lahko v tem primeru država vpliva na kakovost telekomunikacijskih storitev – razpoložljivost, zanesljivost in varnost – ni jasno. Še manj je jasno, kakšna bo kakovost storitev v primeru velikih naravnih in drugih nesreč ter izjemnih stanj? Ob tem je pomenljivo dejstvo, da k pripravi Projekta vzpostavitve državnega računalniškega oblaka vodij informatike iz ministrstev in organov nacionalne varnosti sploh niso bili povabljeni.

Zakon o elektronskih komunikacijah v 123. členu predpisuje kakovost univerzalnih storitev in v 124. členu zahtevano prenosno hitrost podatkovnih omrežij za dostop do interneta. Na podoben način bi veljalo urediti kakovost storitev za potrebe delovanja javnih storitev države in sistemov nacionalne varnosti. Zakon o varstvu pred naravnimi in drugimi nesrečami določa, da je dolžnost države organizacija in vzdrževanje elektronskih komunikacij za potrebe zaščite, reševanja in pomoči do lokalnih skupnosti ter določanje enotnega sistema elektronskih komunikacij. V 53. členu je zapisano, da ima uporaba elektronskih komunikacij za vodenje in prenos podatkov v sistemu opazovanja, obveščanja in alarmiranja prednost pri uporabi vseh vrst elektronskih komunikacij. Kako lahko država sploh uveljavi v zakonu zapisane ukrepe brez neposrednega vpliva na zagotavljanje kakovosti storitev javnih telekomunikacijskih omrežij, še zlasti v bodočem privatnem informacijskem oblaku v katerega naj bi se vključila javna uprava? Pričakovanje, da bo država gradila svoje neodvisno telekomunikacijsko omrežje do vsake od občin, je nerealno. Pomenljiv je spor med Republiko Hrvaško in hrvaškim telekomom, ki je v večinski lasti nemškega telekoma, zaradi načrtovane gradnje državnega optičnega omrežja, ki je zaradi tujega solastništva največjega operaterja postal celo meddržaven.

IV. ZAKLJUČEK

Družba postaja vedno bolj odvisna od informacijskih in komunikacijskih sistemov, ki postajajo vse kompleksnejši in vse bolj nepredvidljivi. Nove tehnologije nam ohranjajo obstoječe in prinašajo nove storitve, vendar prepogosto za ceno slabše kakovosti. Ob velikih naravnih in drugih nesrečah je najpomembnejša razpoložljivost in robustnost storitev, še zlasti storitve za klic v sili na 112. Odgovornost države je, da skrbi ne le za nacionalno, temveč tudi za človeško varnost. Zato je nujno, da zagotavlja nemoteno delovanje kritične infrastrukture, kamor delno spada tudi telekomunikacijska infrastruktura. Eden od ukrepov je tudi koordinacija usklajenega ukrepanja operaterjev javnih telekomunikacijskih omrežij ob velikih in drugih nesrečah.

ZAHVALA

Zahvaljujem se svojemu sodelavcu Grigoriju Krupenku za pomoč pri zbiranju in obdelavi podatkov o klicih na številko 112.

LITERATURA

[1] Andon Batchvarov, Security Issues and Solutions for Voice over IP compared to Circuit Switched Networks, INFOTECH Seminar Advanced Communication Services (ACS), 2004

[2] AKOS, Poročilo o razvoju trga elektronskih komunikacij za drugo četrtletje 2014, 2014

[3] Projekt vzpostavitve državnega računalniškega oblaka – DRO, Investicijski program s študijo izvedbe, verzija 2.0, MNZ, 2014

Boštjan Tavčar je diplomiral na Fakulteti za elektrotehniko v Ljubljani na univerzitetni smeri telekomunikacije. Od leta 1994 je zaposlen na Ministrstvu za obrambo, na Upravi Republike Slovenije za zaščito in reševanje, v zadnjih letih kot vodja Centra za obveščanje Republike Slovenije. Skrbi za uveljavitev in razvoj informacijskih in komunikacijskih sistemov in enotne evropske številke za klic v sili 112. Je avtor aplikacije za klic v sili za gluhe in naglušne WAP112, za katero je Uprava RS za zaščito in reševanje v letu 2009 prejela mednarodno nagrado Evropskega združenja za klic v sili EENA. Predava na Višji strokovni šoli za telekomunikacije, Šolskega centra za pošto ekonomijo in telekomunikacije v Ljubljani in je avtor več strokovnih člankov s področja telekomunikacij, informatike in varstva pred naravnimi in drugimi nesrečami.

DNS kot kritična struktura

Barbara Povše Golob, Benjamin Zwittnig, Arnes

Povzetek — Članek opisuje, kako je DNS vključen v kritično infrastrukturo in kako nacionalni register, ki deluje v okviru Akademske in raziskovalne mreže Slovenije in upravlja tudi z vrhnjim DNS strežnikom za .si, obvladuje tveganja povezana z DNS.

Ključne besede — Register, DNS, kritična infrastruktura

Abstract — Article explains how is DNS involved in national critical infrastructure and approach and some measures for risk managements of DNS at national ccTLD Registry.

Keywords — Registry, DNS, critical infrastructure

I. UVOD

Akademska in raziskovalna mreža Slovenije - Arnes je od leta 1992 s strani IANA (Internet Assigned Names Authority) in Vlade RS pooblaščena organizacija za registracijo domen pod vrhnjo nacionalno domeno .si in upravljanje vrhnjega DNS strežnika za .si.

Obseg nalog Registra za vrhnjo domeno .si je širok. Register zagotavlja možnost registracije domen pod nacionalno domeno. V ta okvir sodi:

- priprava pravil in postopkov za registracijo domen pod .si;
- razvoj, vzdrževanje in nadzor tehničnega sistema za registracijo domen (epp strežnika, portala za registrarje, odjemalca in aplikacije za registrarje);
- sklepanje pogodb z registrarji, redna komunikacija z njimi;
- zastopanje .si v mednarodnih organizacijah;
- spremljanje razvoja in novosti na področju registracije domen, vključno s poznavanjem tehničnih standardov tega področja;
- administracija postopka alternativnega reševanja domenskih sporov (postopek ARDS);
- promocija nacionalne vrhnje domene .si.

Register upravlja tudi vrhnji domenski strežnik (DNS) za nacionalno domeno. Ključne aktivnosti so:

- načrtovanje, nadgradnje in vzdrževanje strojne in programske opreme za primarni in sekundarne domenske strežnike za .si;
- nadgradnje programske opreme ob varnostnih grožnjah;
- nadzor anycast servisa za .si domeno;
- nadzor dosegljivosti in odzivnosti domenskih strežnikov za .si;
- generiranje in DNSSEC podpisovanje .si zone;
- preverjanje in vnos DNS strežnikov za sekundarne domene pod .si;
- vzdrževanje sekundarnih strežnikov za .si;
- zbiranje in obdelava podatkov ter izdelava statistik za .si;
- vzdrževanje in koordinacija strežnikov za reverzne preslikave za Arnesov naslovni prostor v vrhnjih domenah .in-addr.arpa in ip6.arpa.

V nadaljevanju bomo skušali opredeliti upravljanje vrhnjega DNS strežnika v okviru pojma kritične infrastrukture in iskali odgovore na vprašanja:

- Ali upravljamo del kritične infrastrukture (in zakaj)?
- Kje so tveganja in kako jih Register skuša preprečiti?

II. DOMAIN NAME SISTEM (DNS) KOT KRITIČNA INFRASTRUKTURA

A. *Kritična Infrastruktura*

Definicij pojma »kritična infrastruktura« je mnogo in se s časom spreminjajo. Nekoč ločeni sistemi kritične infrastrukture, kot npr. sistemi za preskrbo z vodo, energetika, transportni sistemi, sistemi za preskrbo s hrano, postajajo vse bolj prepleteni in soodvisni. Če se je nekoč kritično infrastrukturo definiralo v nekaj alinejah, se s časom in razvojem tehnologije nabor kritičnih sektorjev širi in je vedno teže definirati tiste, ki niso kritični, saj smo ljudje vedno bolj odvisni od kritične infrastrukture. Poleg tega kritična infrastruktura ni absolutna kategorija, temveč subjektivna, saj številni avtorji pojmujejo kritične infrastrukture kot mreže, ki zagotavljajo prometne, finančne, komunikacijske, preskrbne, elektroenergetske in podobne transakcije, brez katerih ni mogoče zagotavljati normalnega življenja.

V informacijski družbi je vse več zgoraj naštetih kategorij odvisnih od informacijske in komunikacijske tehnologije. Tako bi skorajda lahko rekli, da je v sodobni družbi internet kritična infrastruktura Kritične Infrastrukture.

Delovanje interneta je v grobem odvisno od

- fizične infrastrukture in
- DNS,

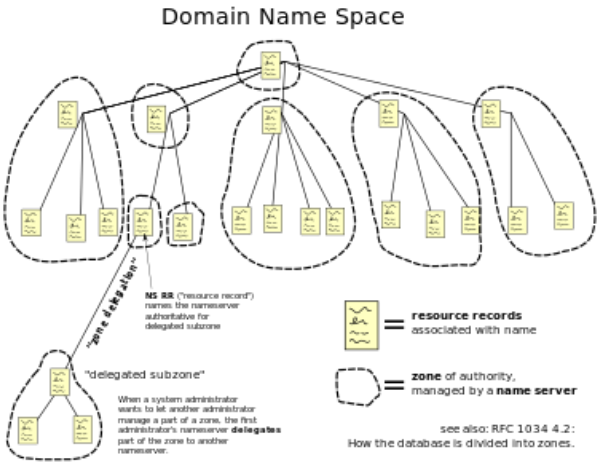
torej je brezhibno delovanje DNS pogoj za delovanje številnih drugih sektorjev in lahko zaključimo, da je DNS del kritične infrastrukture.

B. *Osnove DNS*

V ozadju večine internetnih storitev in aplikacij je DNS. DNS (Domain Name System) je distribuirana baza, ki omogoča lokalno kontrolo posameznih segmentov baze, obenem pa so vsi podatki dosegljivi od vsepovsod s pomočjo sheme strežnik-odjemalec. Osnovna funkcija DNS je pretvorba naslovov IP (npr. 193.2.1.87) v besedne, domenske naslove (*www.register.si*) in tako razni zapisi DNS omogočajo usmerjanje prometa na internetu. Najbolj jasno delovanje sistema domenskih strežnikov pojasni slika 1.

DNS ima torej drevesno strukturo, kjer vsak DNS strežnik »odgovarja« za svoje poddrevo. Govorimo o dveh vrstah DNS strežnikov, avtoritativnih in rekurzivnih. *Avtoritativni* strežniki shranjujejo podatke o domenah, IP naslovih in drugih DNS zapisih za svoje poddrevo. *Rekurzivni* strežniki so tisti, ki odgovarjajo na poizvedbe, podatke pa pridobivajo pri avtoritativnih strežnikih (t.i. DNS resolverji).

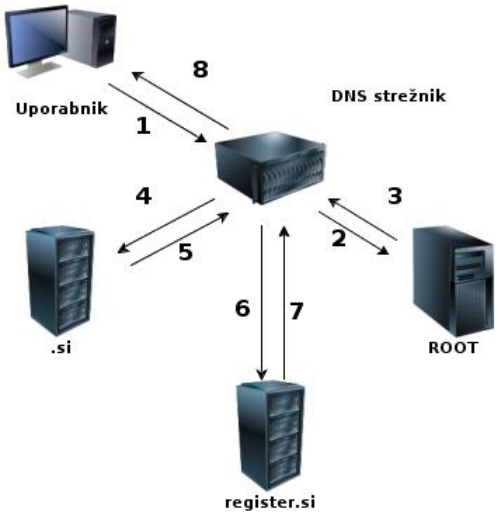
V primarnem DNS strežniku za posamezno domeno se shranjuje celotna kopija DNS baze, vse spremembe in novi zapisi. Sekundarni DNS strežniki podatke pridobivajo izključno od primarnega strežnika in se vanje ne vpisujejo spremembe ali novi zapisi (read only). Vsaka domena ima en primarni in poljubno število (1-255) sekundarnih strežnikov.



Slika 1: Drevesna struktura DNS

Kako poteka sam proces usmerjanja oz. t.i. DNS resolvinga (slika 2)? Uporabnik v spletni iskalnik vpiše, na primer, *www.register.si*. Proces poteka, kot je opisano v nadaljevanju:

- Lokalni strežnik preveri svoj »spomin« (cache), če je pred kratkim že pridobil potrebne podatke za iskano domeno.
- V nasprotnem primeru povpraša enega od root serverjev za avtoritativni strežnik za .si.
- Na avtoritativni strežnik za .si naslovi vprašanje po avtoritativnem strežniku za register.si.
- Ta vrne iskani IP naslov spletnega strežnika.



Slika 2: Proces usmerjanja (DNS resolving)

V svetovnem medmrežju priključene naprave, storitve, aplikacije, … trenutno uporabljajo več 100 milijonov IP naslovov. Vsi DNS strežniki skupaj v vsakem trenutku obdelujejo več 100 milijonov zahtev. Milijoni ljudi vsak dan registrirajo domene, spreminjajo IP naslove, dodajajo in spreminjajo DNS zapise. Na svetu ni baze, ki bi obdelala več zahtev. Obenem z vsemi odgovori se v DNS strežnike dnevno shranijo milijoni novih zapisov in sprememb. Neverjetno pri vsem tem je, da podatki niso shranjeni centralno, ampak je baza razpršena po milijon DNS strežnikih, s stališča uporabnika pa deluje kot enotna baza.

Anycast DNS je storitev, ki povečuje varnost in obenem zagotavlja večjo odzivnost DNS. V Anycast 'oblaku' je veliko strežnikov (node), ki so geografsko razpršeni in so vsi dosegljivi na istem IP naslovu. Z metodo dinamičnega usmerjanja prometa (dynamic routing) so poizvedbe vselej usmerjene do najbližjega strežnika. Tako je izboljšana odzivnost sistema, boljša izkoriščenost in razbremenitev določenih strežnikov.

Storitev bi lahko primerjali s storitvijo klica na 112. Uporabnik, ki kliče na 112, dobi regionalni center. Kljub odpovedi enega centra ostali še vedno delujejo.

Ob morebitnem napadu na anycast 'oblak', se napad avtomatsko lokalizira in prizadane samo napadalcu najbližji strežnik. Za večjo stabilnost uporabljamo več anycast 'oblakov', ki vnašajo potrebno razpršenost in rešujejo problem šibkega člena (single point of failure).

DNS je izredno robusten, stabilen in zmogljiv protokol. Seveda pa se je treba zavedati tudi omejitev. V osnovi je to infrastrukturni protokol in sam po sebi ne more zagotoviti

- zasebnosti (npr. upravljalec rekurzivnega DNS strežnika – najpogosteje ISP – lahko spremlja ves promet stranke),
- avtentikacije,
- integritete podatkov.

Delno slednje pomanjkljivosti odpravlja DNSSEC - varnostna razširitev DNS protokola, ki omogoča avtentikacijo in zagotavlja integriteto DNS podatkov. DNSSEC zagotovi, da odgovor prihaja iz zanesljivega vira in na poti ni prišlo do zlonamerne spremembe. Glede na drevesno strukturo DNS mora biti za popolno zagotovitev integritete DNSSEC implementiran na vseh nivojih. Na ta način se z DNSSEC vzpostavlja veriga zaupanja.

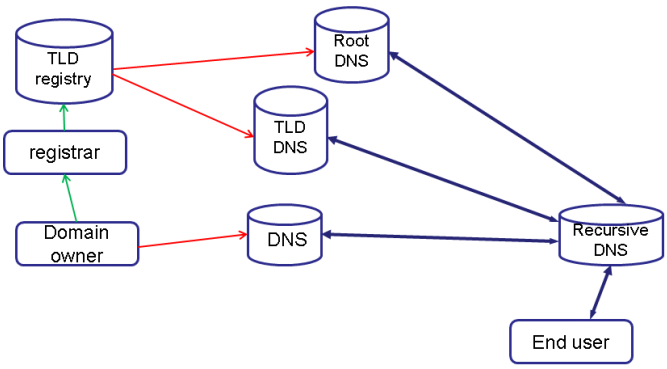
C. Register za .si upravlja s kritično infrastrukturo

i. Shema registra

Zapisi o .si so shranjeni v root zoni, ki jo strežejo root strežniki, torej je delovanje nacionalne .si odvisno od ICANN oz. IANA, ki upravlja root zono. Ker enako velja za vse vrhnje domene, je brezhibno delovanje root strežnikov zagotovljeno in ni neposredno v rokah Registra za .si. Za večjo stabilnost delovanja slovenskega interneta Arnes gostuje tudi Anycast node root strežnika (j.root-servers.net), ki zagotavlja nemoteno delovanje .si domene ob izpadu mednarodnih povezav. Na kaj pa Register .si lahko vpliva?

Slika 3 v grobem predstavlja delovanje registra, vse vpletene subjekte, strežnike in komunikacijske kanale. Ker se Register zaveda, da je brezhibno, neprekinjeno, zanesljivo in stabilno delovanje vrhnje nacionalne domene izredno pomembno, redno opravlja analizo tveganja na vseh področjih delovanja. Pri tem najprej definira potencialna tveganja, oceni njihovo verjetnost in morebitne posledice ter sprejme ukrepe, s katerimi se tveganja zmanjšajo.

V nadaljevanju sledi opis nekaterih možnih tveganj in ukrepov, s katerimi jih register obvladuje.



Slika 3: Delovanje registra

ii. Končni uporabnik

Napad na DNS infrastrukturo se lahko zgodi že na računalniku končnega uporabnika. Različni virusi/malware lahko prestrezajo DNS poizvedbe in postrežejo z napačnimi odgovori. Škoda je omejena na končnega uporabnika. Kljub dejstvu, da ne prizadane velikega števila uporabnikov, je škoda vseeno lahko velika, če gre npr. za napad na DNS zapise banke. Proti tovrstnim grožnjam se lahko borimo z zanesljivimi protivirusnimi programi.

iii. Komunikacija med končnim uporabnikom in DNS strežnikom (resolverjem)

Napadalec lahko prestreza poizvedbe med končnim uporabnikom in rekurzivnim strežnikom, ki ga uporabnik uporablja. V tem primeru lahko pošlje napačen odgovor preden se odzove rekurzivni strežnik. To lahko stori, ker pozna vse ključne identifikacijske parametre DNS poizvedbe. V tem primeru so lahko prizadeti vsi uporabniki, za katere napadalec prestreza promet. Če se napadalec 'vrine' v komunikacijo 'blizu' končnega uporabnika, je napad omejen na majhno število uporabnikov, če pa je 'bližje' rekurzivnemu strežniku, pa je prizadetih lahko zelo veliko uporabnikov. Napad je zelo težko odkriti. Proti napadu se končni uporabniki lahko borijo z namestitvijo DNS strežnika z DNSSEC validacijo na svoj računalnik. Rešitev zaščiti končnega uporabnika le pred potvarjanjem DNS odgovorov za DNSSEC podpisane domene.

iv. Rekurzivni DNS strežnik

Najbolj priljubljena točka napada so rekurzivni strežniki. Napadi so različni. Nekaj je omenjenih v nadaljevanju.

DDOS

Distributed Denial Of Service (Ddos) napadi so največkrat napadi s poplavljanjem. To pomeni, da strežniku napadalec pošlje ogromno količino prometa in s tem prepreči legitimnemu prometu, da bi prišel do strežnika. Posledica napada niso napačni odgovori temveč internetni ‘mrk’. Uporabniki za večino/vse poizvedbe dobijo sporočilo o napaki, da strani niso dosegljive. Za zaščito mora v tem primeru poskrbeti upravljalec rekurzivnega strežnika tako, da zagotovi zadostne kapacitete strežnika in povezav do strežnika ter ustrezno zaščito pred DdoS napadi na svoji infrastrukturi.
Napad prizadane vse uporabnike rekurzivnega strežnika.

ZASTRUPLJANJE MEDPOMNILNIKA

Za zastrupljanje medpomnilnika (cache poisoning) napadalci lahko uporabijo več tehnik. Skupno vsem je, da napadalec poskuša v medpomnilnik DNS strežnika ‘vriniti’ napačne zapise. Napad je zelo težko odkriti. Napad ima lahko zelo obširne posledice in lahko traja precej časa. Če bi napadalcu na primer uspelo vriniti napačen zapis za klik.nlb.si z veliko TTL vrednostjo, bi rekurzivni strežnik toliko časa kot je TTL vračal napačne odgovore za klik.nlb.si. Posledice bi občutili vsi uporabniki tega rekurzivnega strežnika, ki bi v tem času poskušali dostopati do te storitve. Register .si ne more vplivati neposredno na delovanje rekurzivnih strežnikov. .si domeno lahko zaščitimo pred zastrupljanjem medpomnilnika z uporabo DNSSEC tehnologije. Register .si je z DNSSEC tehnologijo podpisal .si in spodbuja uporabo DNSSEC tehnologije na vseh nivojih.

v. Avtoritativni DNS strežnik za .si

Avtoritativne strežnike delimo na primarni strežnik in sekundarne strežnike. Primarni strežnik je strežnik, na katerem urejamo/generiramo zono. Sekundarni strežniki zono 'preberejo' s primarnega strežnika in strežejo podatke iz zone.

Problemi na avtoritativih strežniku so podobni kot na rekurzivnih strežnikih. To po eni strani pomeni, da ne vrnejo odgovora oziroma, da vrnejo napačen odgovor.

Za nevračanje odgovora velja podobno kot v primeru rekurzivnih strežnikov, da je možen vzrok Ddos napad. Register .si se proti Ddos napadom bori z anycast DNS tehnologijo.

Napačne odgovore je potrebno razvrstiti v več kategorij. Za posamezen problem je možnih več vzrokov, ki se lahko med seboj prepletajo:

»Domena ne obstaja (NXDOMAIN)«

Vzrokov za to, da domene ni na DNS strežniku, je lahko več. En od možnih vzrokov je, da se domena ni prenesla (v celoti) na enega ali več sekundarnih strežnikov. Ta težava se je zgodila nemški vrhnji domeni, ko se je zaradi napake preneslo samo pol zone na sekundarne strežnike. Možne so tudi napake registra in registrarjev. Posledice so lahko zelo velike, saj je na primer v nemškem primeru ogromno število domen izginilo z interneta.

»Napaka strežnika (SERVFAIL)«

Tudi za to napako je lahko več vzrokov. Najpogosteje je težava povezana z napakami pri uporabi DNSSEC tehnologije. Možen vzrok so tudi sintaktične napake v zoni in posledično potek (expire) zone na enem ali več sekundarnih strežnikih. Posledice so zelo velike in se v najslabšem primeru lahko zgodi, da celotna .si domena izgine z interneta.

»Napačni podatki«

Podatki so lahko napačni, ker so stari ali pa so bili namerno spremenjeni. Stari podatki so posledica nedelujočega prenosa zone na sekundarne strežnike. Podatke napadalci lahko spremenijo na več načinov. Najmanjše posledice so v primeru vdora na sekundarni strežnik in namerne preusmeritve ene ali več domen. To težavo preprečujemo z uporabo DNSSEC tehnologije. Večjo težavo

predstavlja vdor v sistem registrarja in preusmeritev ene ali več domen iz njegovega portfelja. Register v izogib takim preusmeritvam ponuja storitev registryLock, ki preprečuje spremembo DNS in drugih zapisov za (pomembne) domene, Najbolj problematičen in z največjimi posledicami bi bil vdor v sistem registra in spremembe DNS zapisov za eno ali več domen, Register se proti tovrstnim grožnjam bori s skrbnim spremljanjem varnostnih groženj in z omejenim dostopom do sistemov registra (npr. IP whitelisting za dostop registrarjev do sistema). Aplikacije, ki jih uporablja sistem za registracijo domen, ne dostopajo direktno do baze domen. Prav tako imamo dodatne varnostne ukrepe ob generiranju .si zone datoteke, ki neodvisno preverijo v zone datoteki za morebitnimi sledmi vdora. V primeru odkritja 'čudnih' zapisov se nova zone datoteka ne objavi.

Register .si podrobno spremlja delovanje avtoritativnih strežnikov za .si in takoj alarmira upravljalce sistema v primeru odkritih težav. Nedelovanje oziroma napačno delovanje avtoritativnih strežnikov za .si ima lahko zelo velike posledice na vse slovenske uporabnike interneta in tudi širše.

D. *Blokiranje domen na nivoju registra = poseg v kritično infrastrukturo*

i. *Blokiranje domen*

Blokada domene je oblika filtriranja na nivoju DNS resolucije, torej preslikave med IP naslovom in domeno na način, da prepreči odgovor (npr. stran ni dosegljiva) ali celo preusmeri iskalca na drugo spletno stran. V slednjem primeru gre za preusmeritev domene (redirection). Blokada domene se zagotovi s spremembo DNS zapisov na rekurzivnih strežnikih, obenem pa se za to domeno prepreči, da bi rekurzivni strežnik spraševal avtoritativne strežnike za prave podatke za to domeno. Blokada se lahko naredi na več nivojih.

DNS ima dve ključni funkciji. Prva je že omenjeno človeku prijazno omogočanje dostopa do številnih internet storitev in aplikacij na osnovi besednih naslovov. Druga funkcija je uporabniku manj vidna, zato pa nič manj pomembna. Večina storitev za svoje delovanje potrebuje DNS: elektronska pošta, instantna sporočila, internet telefonija, … S stališča omrežne arhitekture je poseganje v storitve na nivoju infrastrukture in torej daleč od dejanskega cilja blokade (tipično vsebine spletne strani) nevarno predvsem zaradi nepredvidenih posledic, ki jih ima tak poseg na povezane storitve. Zato je s tehničnega stališča vsako filtriranje učinkovito in proporcionalno le, če se implementira čim bližje cilju (vsebini ali uporabniku).

ii. *Blokiranje domen ni učinkovito*

Preprečevanje dostopa do vsebine preko blokiranja domene ni smiselno in učinkovito. Vsebina, ki je cilj blokade, ostaja na spletu in tako še vedno dosegljiva bodisi neposredno preko IP naslova, na drugi domeni, preko anonimnih proxy strežnikov, lahko pa tudi preko posebnih portalov, ki shranjujejo vsebino. Poleg tega lahko uporabniki preko VPN kanalov prikrijejo svojo lokacijo in na ta način obidejo nacionalno zakonodajo ali pa uporabijo DNS resolverje v tujini, ki ne podležejo lokalni zakonodaji. V primeru, da se sodni nalog za blokado nanaša na konkretnega ponudnika, bo že menjava ISP-ja uporabniku znova omogočila dostop do vsebin.

iii. *Neželene posledice blokiranja na nivoju Registra*

Registri vrhnjih domen, še posebej nacionalnih, se vse pogosteje srečujemo z zahtevami sodnih organov, inšpekcij, raznih upravnih in državnih organov in odvetniških pisarn po blokadi določene domene zaradi neprimernih vsebin, ki se nahajajo na spletni strani pod to domeno.

Že prej je bilo obrazloženo, zakaj je blokada na nivoju registra neprimerna. Ukrep ni le neprimeren, temveč nesorazmeren. Blokada domene *primer.si* ne pomeni le nedostopnosti spletne strani *www.primer.si*, povzroči nedostopnost vseh ostalih storitev, vezanih na to domeno, ki so povsem legalni, npr. internet telefonije, elektronske pošte *johanca@primer.si* ali delovanja internetnega radia *radio.primer.si* in spletne trgovine *trgovina.primer.si.* Posledica blokade je torej lahko tudi velika poslovna škoda subjektov, ki opravljajo svojo dejavnost povsem legalno in odškodninski zahtevki le-teh bodo upravičeni in na sodišču uspešni. Bo stroške nosil Register?

Žal se tudi slovenski register sooča z zahtevami po preusmeritvah in blokadah brez pravne osnove. Zahteva po blokadi pomeni poseg v kritično infrastrukturo in brez poznavanja delovanja DNS imajo te zahteve lahko širše in neželene posledice.

III. ZAKLJUČEK

Register za nacionalno vrhnjo domeno se zaveda pomembnosti svoje naloge in tveganj, po najboljših močeh z različnimi ukrepi skrbi za stabilno, zanesljivo, varno in neprekinjeno delovanje interneta pod vrhnjo domeno .si.

Že več let opozarjamo resorno ministrstvo na kadrovsko podhranjenost nacionalnega registra, ki v tem trenutku šteje 6 redno zaposlenih. Podatki evropskega združenja nacionalnih registrov CENTR kažejo, da je to bistveno manj, kot imajo zaposlenih drugi primerljivi evropski nacionalni registri, saj je povprečno število zaposlenih v registrih z do 500.000 domenami 15 (torej skoraj 3 krat več!).

Posledica kadrovske podhranjenosti je tudi povečana obremenjenost zaposlenih, ki lahko vodi v napake z obširnimi posledicami.

Register je del kritične infrastrukture, od katere je odvisno delovanje slovenskega interneta. Nedelovanje bo imelo obsežne posledice na vseh področjih: gospodarstvo, sociala, zdravstvo, …

Ali si Slovenija to res lahko privošči?

LITERATURA

[1] Iztok Prezelj, Nacionalna kritična infrastruktura v Republiki Sloveniji. Teorija in praksa, let 46, 4/2009

[2] https://centr.org/CENTR-Paper-Domain_blocking

[3] Interni dokumenti Registra za .si in www.register.si

[4] Slika DNS resolvinga: http://en.wikipedia.org/wiki/Domain_Name_System

Barbara Povše Golob je na Arnesu zaposlena že od leta 1994. Je vodja registra domen pod .si ter predstavnica Arnesa v svetu evropskih registrov nacionalnih vrhnjih domen – CENTR od njegove ustanovitve naprej.

Benjamin Zwittnig je na Arnesu zaposlen od leta 1992. V okviru svojega dela je pokrival široko paleto omrežnih in spletnih storitev, od leta 2000 pa je vključen v aktivnosti nacionalnega registra za .si domeno, kar vključuje storitve registra za registrarje, operacije ccTLD DNS, nadzor in testiranje.

Zemeljsko magnetno polje in njegov vpliv na telekomunikacije

Rudi Čop, Zavod Terra Viva, Sečovlje

Povzetek – S stalnimi meritvami sprememb zemeljskega magnetnega polja ter z obdelavo in razlago rezultatov teh meritev spremljamo dogajanja v celotnem prostoru med Soncem in Zemljo. Take meritve, ki med drugim omogočajo tudi izračunavanje lokalnega geomagnetnega indeksa K, smo organizirali na geomagnetnem observatoriju IMO (INTERMAGNET Observatory) v slovenskem delu Istre. Izračun indeksa K priporoča mednarodna organizacija IAGA (International Association for Geomagnetism and Aeronomy) za vsakodnevno opisovanje aktivnosti geomagnetnega polja na delu površine Zemlje, ki ga tak observatorij pokriva. V prispevku so predstavljena izhodišča pri izbiri kraja za postavitev observatorija IMO PIA (Piran, Slovenia), ki je vključen v mednarodno informacijsko mrežo INTERMAGNET (INTErnational Real-time MAGnetic observatory NETwork) za izmenjavo minutnih merilnih podatkov o spremembah zemeljskega magnetnega polja v skoraj realnem času. Predstavljeni so nekateri merilni rezultati s tega observatorija in vplivi sprememb zemeljskega magnetnega polja na naše vsakdanje življenje kot tudi na telekomunikacije.

Ključne besede - Geomagnetni observatorij, ozemlje Slovenije, spremembe zemeljskega magnetnega polja, vpliv na naše vsakdanje življenje.

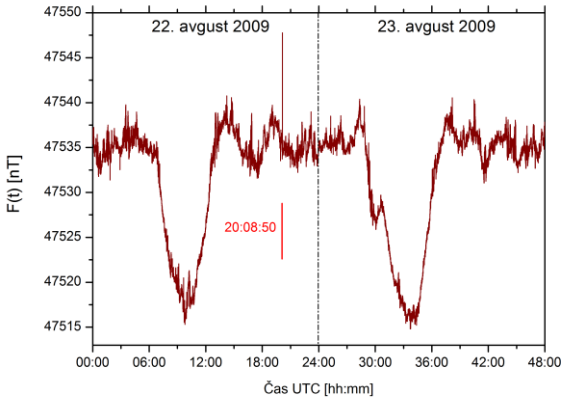
Abstract – It is possible to detect the conditions in the space between the Sun and the Earth with continuous measurements of variations of geomagnetic field, processing the results and interpretations of them. We organized such type of measurements in Slovenian part of Istria on the INTERMAGNET Observatory - IMO. These measurements offer us also the possibility to calculate the local geomagnetic index K. Calculation of geomagnetic index K is recommended by International Association for Geomagnetism and Aeronomy - IAGA. In this article are presented the starting points of the construction of the IMO PIA (Piran, Slovenia). This observatory is included in the international network INTERMAGNET (INTErnational Real-time MAGnetic observatory NETwork) for exchange the minute date of variation of geomagnetic field in near real time. There are also presented some measurements from this observatory and some influences of variation of geomagnetic field on our everyday life and also on the telecommunication as well.

Key words – Geomagnetic observatory, Slovenia, variations of geomagnetic field, impact on our everyday life.

I. GEOMAGNETNI OBSERVATORIJ V SLOVENIJI

Geomagnetni observatorij je referenčno mesto za geomagnetne meritve na ozemlju, ki ga tak observatorij pokriva. Na sedanji stopnji razvoja merilne tehnike je to območje široko za okoli pet minut hoda Sonca. Mora biti postavljen na skrbno izbranem mestu, ki ustreza tudi mednarodnim priporočilom [1]. Običajno je izbrano mesto kompromisna rešitev med priporočili in danimi možnostmi. Da se lahko observatorij vključi v obstoječo mednarodno informacijsko mrežo INTERMAGNET mora biti tudi opremljen po ustreznih priporočilih [2]. Šele ta mednarodna povezava daje geomagnetnemu observatoriju pravo veljavo.

Geomagnetnemu observatoriju priznava usposobljenost za opravljanje geomagnetnih meritev (slika 1) njegova vključitev v mednarodno informacijsko mrežo: a) zagotavlja opremljenost in delovanje observatorija po priporočilih mednarodnih organizacij IAGA (International Association of Geomagnetism and Aeronomy) in INTERMAGNET, b) omogoča stalno preverjanje delovanja observatorija, c) redno preverjanje njegove merilne opreme in d) redno izobraževanje sodelavcev observatorija ter e) pomoč pri modernizaciji observatorija.



Slika 1: Spremembe absolutnih vrednosti vektorja zemeljskega magnetnega polja F(t) v dveh zaporednih geomagnetno mirnih dnevih poleti 2009, izmerjene na Gori nad Ajdovščino z registracijo prehoda nevihtne fronte in udara strele

Sistematično iskanje primernega mesta za izhodiščne meritve zemeljskega magnetnega polja na ozemlju Slovenije smo začeli v letu 2007 [3, 4]. Poleg mednarodnih priporočil smo pri iskanju primernega mesta za postavitev observatorija upoštevali tudi geološke, seizmološke in hidrološke posebnosti našega ozemlja. V naših razmerah tak observatorij ogrožajo vandalizmi, gozdni požari in atmosferske prenapetosti [5]. V februarju 2014 smo pri vasi Sv. Peter nad Sečovljami začeli s pripravami za postavitev geofizikalnega observatorija Sikuri. V vozlišče INTERMAGNET v Edinburgu je bil vključen v prvi polovici decembra 2014 kot testni observatorij (TEST Observatory) s kodo IAGA: PIA (Piran, Slovenia). Merilni podatki, podani v kodi ASCII, so za prenos oblikovani v formatu IMFV1.2N [2] oziroma v novejšem formatu IAGA 2002 [6].

Geomagnetni observatorij IMO PIA smo postavili zato, da lahko spremljamo razmere v zgornjih plasteh atmosfere in v medplanetarnem prostoru v bližini Zemlje, ugotavljamo indukcijo v zemeljski skorji in plašču ter proučujemo razmere v tekoči sredici Zemlje in v njenem trdem jedru [7, 8]. Povezave med magnetosfero, ionosfero in zemeljsko atmosfero so nelinearne in še ne dovolj raziskane. Glavni

razlog je prekratko obdobje vseh do sedaj opravljenih meritev glede na dolžino sončnih ciklov [9, 10].

Geomagnetni observatorij IMO PIA je materialna osnova za razvoj znanja o geomagnetizmu v Sloveniji. Geomagnetizem je del geofizike, najbolj sofisticiranem delu geologije, vede o planetu Zemlja. Znanje iz tega področja se danes neposredno uporablja na več področjih našega vsakdanjega življenja [11, 12]. Poleg telekomunikacij so ta področja še: radijska in magnetna navigacija, energetika, geologija z rudarstvom [13, 14], geotehnika, seizmologija, meteorologija [15], ekologija, klimatologija [16, 17], arheologija, promet, medicina [18] in biologija [19, 20]. Sodobne tehnologije so odvisne od stanja v magnetosferi, v ionosferi in v zemeljski skorji tako, kot ni bila še nobena v predhodnih razvojnih stopnjah človeške civilizacije.

II. RAZELEKTRITVE V IONOSFERI

Vpliv vesolja na Zemljo je poleg vpada meteorjev, polarnih sijev in oblakov v mezosferi viden še kot tlenje svetlobe v ionosferi in razelektritve v njej. Ionosfera ni posebna plast zemeljske atmosfere, temveč so to plasti v njej, od katerih se odbijajo radijski valovi in svoje lastnosti spreminjajo tekom celega dneva in tekom letnih časov [21, 22]. Zaradi ionizirajočega sevanja Sonca, ki razstavlja molekule zraka pri ustrezno nizkem zračnem tlaku, ionosfero sestavlja hladna plazma. V njej obstajajo prosti elektroni ob naelektrenih molekulah, ki težko dosežejo rekombinacijo. Zaradi naelektrenih delcev v ionosferi nastajajo v zgornjih plasteh atmosfere električni toki.

Razelektritve v ionosferi so vezane na lastnosti hladne plazme. Te vrste razelektritev ali dogodki TLE (Transient Luminous Event) obsegajo različne oblike razelektritev v zgornjih plasteh atmosfere in so podobne razelektritvam v fluorescentnih cevih. Nastajajo visoko nad nevihtnimi oblaki običajno v zaključnem obdobju neviht. Sprožijo jih strele med oblaki in zemeljsko površino s pozitivnimi nosilci električnega naboja. S prostim očesom lahko dogodke TLE opazimo zelo redko in to le v izjemnih okoliščinah, ko je nad najbolj aktivnimi deli nevihtnih oblakov prosta vidljivost. Dogodki TLE so dobro dokumentirani šele v zadnjih dveh desetletjih kot posledica razvoja dovolj hitrih video kamer za nočno snemanje. S pomočjo opazovalnih satelitov, ki krožijo okoli Zemlje, pa je bilo ugotovljeno, da je teh dogodkov v enem letu preko dva milijona [23, 24].

Razelektritve v ionosferi se dogajajo več kot petkrat višje od višine nevihtnih oblakov, ki so pod vplivom močne vertikalne konvekcije zraka v troposferi in obenem tudi slabšega horizontalnega gibanja zraka v stratosferi. Te skupine nevihtnih oblakov MCS (mesoscale convective system) so sicer večje kot oblaki lokalnih neviht, vendar manjše kot ekstremni tropski cikloni. V Evropi se najpogosteje pojavljajo v drugi polovici avgusta in v septembru in to v območju zahodnega dela Sredozemskega morja (slika 2). Njihova najbolj običajna smer potovanja je vzhodno severovzhodno in to v popoldanskem času ter v povprečju obsegajo okoli 9000 km^2 [25].

Slika 2: Razelektritev v ionosferi nad jugozahodnim delom Slovenije, posneta na observatoriju GEOS pri Weiningenu v Švici 9.11.2013 ob 17:44:23 UTC [26]

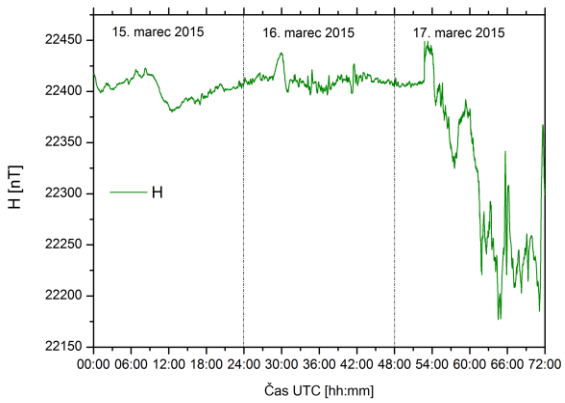
Raziskave v zadnjem desetletju prejšnjega stoletja so pokazale, da nastajajo ob razelektritvah v ionosferi tudi ekstremno dolgi elektromagnetni valovi ELF (extremely low frequency) v frekvenčnem področju od 3 Hz do 300 Hz [27, 28]. Zaradi resonančnega pojava se valovi ELF ojačijo v naravnem valovodu med zemeljsko površino in ionosfero [29, 30]. Zato ti valovi obstajajo dlje kot razelektritve v ionosferi in tudi ne pojenjajo toliko z oddaljevanjem od njihovega izvora. Na osnovi proučevanja ionosferskih razelektritev s pomočjo sprejemnikov ELF je bilo ugotovljeno, da se intenzivnost teh razelektritev spreminja s sončnimi cikli [31].

Naše proučevanje razelektritev v ionosferi je nadaljevanje dela na področju zaščite magnetometrov pred atmosferskimi razelektritvami [5]. Rezultati našega dela se kažejo v observatoriju IMO PIA: a) uspešna izbira mesta njegove postavitve, b) njegova enkratna oblika, c) nova generacija triosnih magnetometrov fluxgate z vgrajeno prenapetostno zaščito, ki se preizkuša na tem observatoriju.

III. SPREMEMBE V MAGNETOSFERI IN V ZGORNJIH PLASTEH OZRAČJA

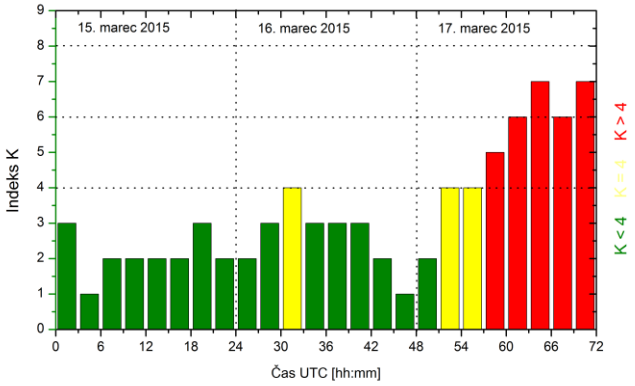
Za vsakodnevno opisovanje aktivnosti zemeljskega magnetnega polja mednarodna organizacija IAGA priporoča geomagnetni indeks K. Indeks K določamo na osnovi zveznih meritev na geomagnetnih observatorijih na površini Zemlje (Slika 3). To so meritve aktivnosti električnih tokov v ionosferi in magnetosferi ter motenj, ki jih ti tokovi povzročajo [32]. Iz teh meritev izhaja indeks geomagnetne aktivnosti K, ki sloni na skalarni matriki, s katero se popisuje velikost odstopanja od srednjega geomagnetno mirnega dne [33].

Za izračunavanje geomagnetnega indeksa K je izbran tri urni interval [34, 35]. Tak interval se je izkazal za primernega zato, ker so v njem zajete geomagnetne motnje, ki trajajo od ene do dveh ur in ki je dovolj kratek, da se z njim lahko loči dva zaporedna dogodka, nastala tekom dneva (slika 4). Od začetka šestdesetih let prejšnjega stoletja se geomagnetni indeks K lahko določa le iz obeh horizontalnih komponent. Komponenta Z je namreč najbolj pod vplivom nenaravnih motenj zemeljskega magnetnega polja.



Slika 3: Horizontalna komponenta zemeljskega magnetnega polja H [nT] izmerjena na IMO PIA v treh zaporednih dnevih

Stopnje v logaritmični skali geomagnetnega indeksa K odražajo velikost motenj. Te motnje se, od najnižje stopnje K = 0 do najvišje stopnje K = 9, po magnitudi med seboj razlikujejo za velikostni razred sto. Z geomagnetnim indeksom K večjim od vrednosti 4 se opisujejo geomagnetne nevihte. V izjemnih primerih lahko njihove učinke opazujemo tudi v nižjih zemljepisnih širinah (slika 5). Najpogostejši vzrok za nastanek geomagnetnih neviht so izbruhi v koroni Sonca CME (coronal mass ejection), ki so tudi izvor sevanja elementarnih delcev velikih energij SEP (solar energetic particles). Izbruhi v koroni Sonca imajo svoj izvor v globljih plasteh Sonca in jih lahko spremljajo tudi bliski v sončnih pegah [36, 37]. Na geomagnetno polje Zemlje in s tem tudi na njene plasti zraka vpliva sončni veter, ki izhaja iz Sonca. Njegova povprečna hitrost je med 300 in 800 km/s. To je tok elementarnih delcev, ki v obliki plazme iz sončevih zunanjih plasti potujejo po celotnem osončju in pri tem zadenejo tudi Zemljo. Sestavljajo ga: stalni tok spremenljive hitrosti, ki izhaja iz tokovnic kromosfere, povečan tok, ki izhaja iz lukenj v koroni Sonca, in impulzi ob izbruhih CME. Danes je vpliv Sonca na Zemljo sprejeto dejstvo, v fazi intenzivnega raziskovanja pa so energijske povezave med vplivom Sonca na magnetno polje Zemlje in njeno atmosfero [38, 39].



Slika 4: Vrednosti lokalnega geomagnetnega indeksa K za Slovenijo za tri zaporedne dneve

Izhodiščni indeks v geomagnetizmu in aeronomiji, znanosti o zgornjih plasteh atmosfere, je danes planetarni geomagnetni indeks Kp. Vrednost tega indeksa se napoveduje in nato tudi postprocesira na osnovi meritev na izbranih referenčnih geomagnetnih observatorijih [32]. Poleg stanja celotnega zemeljskega magnetnega polja za širše področje dobro predstavlja tudi razmere v ionosferi (ionspheric storms). Za opis razmer v ionosferi na ožjem področju pa je bolj primeren lokalni indeks K iz najbližjega geomagnetnega observatorija.

Slika 5: Polarni sij v Sloveniji 17. marca 2015 ob 23:00:06 UTC fotografiran iz Jošta nad Kranjem v azimutni smeri 88,7° [40]

IV. PRENOS PODATKOV PO OMREŽJU MOBILNE TELEFONIJE

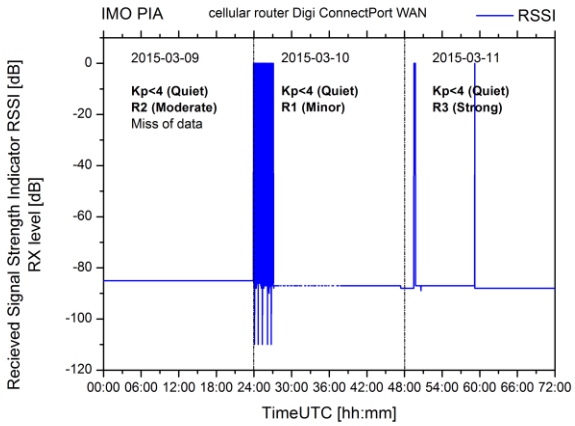
Za postavitev sodobnega geomagnetnega observatorija obstajajo priporočila, vendar so vsa osredotočena na merilne instrumente, meritve in obdelavo merilnih podatkov. Zelo skopa pa so ta navodila glede zajemanja in prenosa merilnih podatkov ter zagotavljanja varnega in zanesljivega obratovanja [1, 41]. Za sodoben geomagnetni observatorij IMO pa je zanesljiva in robustna telemetrija ne samo potrebna za prenos merilnih podatkov, temveč tudi za daljinski nadzor delovanja merilnih instrumentov in celotnega observatorija z namenom, da se zagotovi zanesljiva in neprekinjena registracija vrednosti komponent zemeljskega magnetnega polja.

Izhodiščni parametri pri našem razvoju telemetrije so bili: zanesljivost prenosa merilnih podatkov in stroški tega prenosa, cena in dosegljivost opreme ter stroški vzdrževanja in možnost nadaljnjega razvoja sistema [42]. Ocenjena je bila količina merilnih podatkov v časovni enoti in določeni so bili še dodatni pogoji, ki so se nanašali predvsem na zapisovalnik podatkov (Data Logger).

Za prenos merilnih podatkov od geomagnetnega observatorija do strežnika uporabljamo brezžični paketni prenos podatkov. Cenovno ugodna tehnologija omogoča tak prenos, ki ponuja pri manjših stroških za prenos podatkov tudi povečano varnost pred atmosferskimi prenapetostmi. Je pa tak prenos omejen tako po hitrosti kot tudi po količini prenesenih informacij. Izkoriščamo že obstoječe brezžično omrežje ponudnika storitve za digitalno komunikacijo. Pri uporabi takega načina prenosa merilnih podatkov smo v letu 2014 začeli registrirati tudi vrednost signala RSSI (Received Signal Strength Indication, RX level).

Ker se mikrovalovi v prostoru širijo premočrtno, je njihov doseg odvisen od vremenskih razmer vzdolž poti njihovega širjenja. Hitrost njihovega širjenja je odvisna od temperature in vlažnosti zraka ter zračnega tlaka [43]. Na širjenje mikrovalov v troposferi ne vplivajo samo lastnosti zraka, padavin in primesi v njem, temveč tudi neposredno sevanje Sonca. Dosedanje meritve vrednosti signala RSSI na IMO

PIA (Slika 6) so v korelaciji s spremembo hitrosti sončnega vetra in gostoto elementarnih delcev v njem. Spremembe vrednosti signala RSSI so le v delni korelaciji s planetarnim geomagnetnim indeksom Kp in planetarno oceno širjenja radijskih signalov R (radio blackout). Dosedanje meritve vrednosti signala RSSI kažejo, da je način širjenja mikrovalov v troposferi lokalnega značaja. Ker so na razpolago le minutni merilni podatki o vrednosti signala RSSI, so za podrobnejše aeronomske meritve te meritve pregrobe. Zato bi jih morali izboljšati s primernejšimi merilnimi instrumenti za merjenje širjenja radijskih valov in mikrovalov skozi troposfero in ostale zračne plasti [44, 45].



Slika 6: Jakost sprejemnega signala RX [dB] modema za komunikacijo po omrežju mobilne telefonije na IMO PIA v treh zaporednih dnevih

V. ZAKLJUČEK

V nadaljevanju našega dela imamo zastavljene naslednje cilje:

1. Širjenje znanja iz področja geomagnetizma in aeronomije predvsem na področjih pomembnih za vsakdanje življenje. Pridobivanje znanj na področju geomagnetizma in aeronomije je v zadnjih petdesetih letih nadpovprečno hitro [46]. Poleg tega pa se preko polovice vseh meritev in razvojnih projektov odvija v Evropi.
2. Prehod iz TEST Observatory IMO v polnopravni Observatory IMO.
3. Doseči samozadostnost in povečati zanesljivosti delovanja observatorija.

Že prehod iz testne oblike v obliko rednega delovanja observatorija v mednarodni informacijski mreži INTERMAGNET zahteva vsaj formalno vključitev observatorija v ustrezni večji sistem v Republiki Sloveniji. Še bolj pa je to vključevanje pomembno za dosego samozadostnosti in povečanje zanesljivosti delovanja observatorija. Ta pogoj izhaja iz sedanje oblike organizacije vseh geomagnetnih observatorijev IMO, ki imajo le po dva verificirana merilca. Zaradi premajhnega števila raziskovalcev na observatoriju se mora observatorij obvezno vključevati tudi v raziskave s partnerji izven države in si v mednarodni skupnosti najti svoje lastno razvojno-raziskovalno mesto.

O smeri nadaljnjega razvoja observatorija odloča predvsem njegovo vključevanje v večje sisteme ter v razvojne in aplikativne projekte doma in v tujini. Take usmeritve bi bile lahko: a) objavljanje lokalnega indeksa K (telekomunikacije, radijska navigacija), b) meritev telurskih tokov (ozemljitve, daljnovodi, kablovodi), c) meritev impulzov geomagnetnega polja (telekomunikacije, medicina) in d) meritev lastnosti ionosfere (telekomunikacije, radijska navigacija).

ZAHVALA

Zahvaljujem se kolegu Petru Reismanu za pregled celotnega besedila in kolegu Janezu Forteju za dopolnitev povzetka tega članka.

LITERATURA

[1] Jerzy Jankowski, Christian Sucksdorff, Guide for Magnetic Measurements and Observatory Practice. Boulder (US): International Association of Geomagnetism and Aeronomy IAGA, 1996.

[2] INTERMAGNET Technical Reference Manual. Version 4.6. Edited by: Benoît St-Louis. Edinburgh (UK): British Geological Survey, 2012.

[3] Dejan Paliska, Rudi Čop, Daša Fabjan, The Use of GIS-based Spatial Multi-criteria Evaluation in the Selection Process for the New Slovenian Geomagnetic Observatory Site. *Annales Ser. hist. nat.* 2010, **20** (1), 1-8.

[4] Rudi Čop, Gradnja geomagnetnega observatorija pod Sinjim vrhom nad Ajdovščino. Urednik Miran Kuhar. *Raziskave s področja geodezije in geofizike 2010*. Zbornik predavanj. Ljubljana: Fakulteta za gradbeništvo in geodezijo, 2011, 59-64.

[5] R. Čop, G. Milev, D. Deželjin, J. Kosmač, Protection against lightning at a geomagnetic observatory. *Geosci. Instrum. Method. Data Syst.*, 2014, **3**, 135–141.

[6] Susan McLean, *IAGA2002 data Exchange Format* [online]. IAGA Division Working Group V-DAT; Geomagnetic Data and Indices, Revised 7 October 2011 [viewed 25 February 2015]. Available from: http://www.ngdc.noaa.gov/IAGA/vdat/iagaformat.html

[7] Jeffrey J. Love, K. J. Remick, Magnetic Indices. *Encyclopedia of Geomagnetism and Paleomagnetism.* Dordrecht (Netherlands): Springer, 2007, 509-512.

[8] S. Chapman, A. T. Price, The Electric and Magnetic State of the Interior of the Earth, as Inferred from Terrestrial Magnetic Variations. *Philosophical Transactions of the Royal Society of London, Series A*, 1930, 229, 427-460.

[9] K. G. Rangarajan, M. L. Barreto, Long term variability in solar wind velocity and IMF intensity and the relationship between solar wind parameters and geomagnetic activity. *Earth Planets Space*, 2000, **52**, 121–132.

[10] Elena Saiz, et al. Geomagnetic response to solar and interplanetary disturbances. *J. Space Weather Space Clim.*, 2013, **3** (A26), 1-20.

[11] James A. Marusek, *Solar Storm Threat Analysis.* Bloomfield (IN, US): Impact, 2007.

[12] *Geomagnetic Storms*. OECD/IFP Futures Project on "Future Global Shocks". Burlington (MA, US); Arlington (VA, US): CENTRA Technology, 2011.

[13] Benny Poedjono, et al. Using *Geomagnetic Referencing Technology for Precise Wellbore Placement.* AADE-11-NTCE-13. San Antonio (US): American Association of Drilling Engineers AADS, 2011.

[14] Andrew Buchanan, et al. Geomagnetic Referencing – The Real-Time Compass for Directional Drilling. *Oielfield Review*, 2013, **25** (3), 32-47.

[15] Rudi Čop, Damir Deželjin, Lokalne spremembe zemeljskega magnetnega polja zaradi prehoda vremenske fronte. *Raziskave s področja geodezije in geofizike 2013.* Zbornik del. Urednik Miran Kuhar. Ljubljana: Fakulteta za gradbeništvo in geodezijo, 2014, 77-83.

[16] MARSH, Nigel. SVENSMARK, Henrik. Cosmic rays, clouds, and climate. *Space Science Reviews*, 2000, **00**, 1–16.

[17] Freddy Christiansen, Joanna D. Haigh, Henrik Lundstedt, *Influence of Solar Activity Cycles on Earth's Climate.* ISAC Final Report; Scientific Report 2/2007. Copenhagen (DK): Danish National Space Center, 2007.

[18] Damir Deželjin, Rudi Čop, IT System for Alarming of Possible Health Risks Caused by Geomagnetic Storms. *Global Telemedicine and eHealth Updates: Knowledge Resorces*, 2013, **6**, 512-515.

[19] Richard P. Blakemore, Magnetotactic bacteria. Annual Reviews of Microbiology, 1982, **36**, 217-238.

[20] Tadashi Matsunaga, et al. Molecular analysis of magnetotactic bacteria and development of functional bacterial magnetic particles for nano-biotechnology. *Trends Biotechnology*, 2007, **25** (4):182-188.

[21] *Handbook of Geophysics and the Space Environment*. Scientific editor Adolph S. Jursa. Springfield (VA, US): United States Air Force; Air Force Systems Command; Air Force Geophysics Laboratory, 1985.

[22] Dave Anderson, Tim Fuller-Rowell, *The Ionosphere*. SE-14. Boulder (US): Space Environmental Center, 1999.
[23] Earle R. William, Sprites, Elves, and Glow discharge Tubes. *Physics Today*, November 2001, 1-7.
[24] Alfred B. Chen, et al. Global distributions and occurrence rates of transient luminous events. *Journal of Geophysical Research*, 2008, **113**, A08306, doi:10.1029/ 2008JA013101.
[25] C. Morel, S. Senesi, A climatology of mesoscale convective systems over Europe using satellite infrared imagery. II: Characteristics of European mesoscale convective systems. *Quartaly Journal of the Royal Meteoroogical Sciety*, 2002, **128**, 1973–1995.
[26] Roger Spinner, *AW: Request*. From: roger.spinner@geos-weiningen.ch, To: rudi@artal.si. Wed, Sep 3, 2014 at 8:23 AM. Available from: Internet.
[27] R. Barr, Jones D. Llanwyn, J. C. Rodger, ELF and VLF radio waves. *Journal of Atmospheric and Solar-Terrestrial Physics*, 2000, **62**, 1689-1718.
[28] S. U. Inan, A. S. Cummer, A. R. Marshall, A survey of ELF and VLF research on lightning-ionosphere interactions and causative discharges. *Journal of Geophysical Research*, 2010, **115**, A00E36, doi:10.1029/2009JA014775.
[29] Devendraa Siingh, et al. *Thunderstorms, lightning, sprites and magnetospheric whistler-mode radio waves.* Varanasi (India): Banaras Hindu University, Department of Physics, Atmospheric Research Laboratory, 2009.
[30] A. Ohkubo, et al. VLF/ELF sferic evidence for in-cloud discharge activity producing sprites. *Geophysical Research Letters*, 2005, **32**, L04812, doi:10.1029/ 2004GL021943.
[31] Mitsuteru Sato. *Global Lightning and Sprite Activities and Their Solar Activity Dependences.* Dissertation. Sendai (Japan): Tohoku University; Depatment of Geophysics; Graduate School of Science, 2003.
[32] Jeffrey J. Love, Magnetic monitoring of Earth and space. *Physics Today*, 2008, **61**, 31–37.
[33] P. N. Mayaud, *Derivation, Meaning, and Use of Geomagnetic Indices.* Gophysical monograph 22. Washington (DC, US): American Geophisical Union, 1980.
[34] G. K. Randarajan, Indices of Geomagnetic Activity. *Geomagnetism. Volume 3*. Edited by J. A. Jacobs. London: Academic Press, 1989, p.323-384.
[35] J. Bartels, N. H. Heck, H. F. Johnston, Geomagnetic three hour-range indices for the years 1938 and 1939, *Terrestrial Magnetism and Atmospheric Electricity*, 1940, **45**, 309–337.
[36] Rudi Čop, et al. Magnetne nevihte in njihov vpliv na navigacijo. *Raziskave s področja geodezije in geofizike 2007*. Zbornik predavanj. Urednik Miran Kuhar. Ljubljana: Fakulteta za gradbeništvo in geodezijo, 2008, 71-80.
[37] Karl-Heinz Glassmeier, Heinrich Soffel, Jörg F.W. Negendank, *Geomagnetic Field Variations.* Berlin; Heidelberg: Springer-Verlag, 2009.
[38] *The Sun and Heliosphere in Three Dimensions.* Report of the NASA Science Definition Team for STEREO Mission. Laurel (US): Johns Hopkins University Applied Physics Laboratory, 1997.
[39] *Reconnection of Magnetic Fields; Magnetohydrodynamics and Collisionless Theory and Observations.* Edited by J. Birn and E. R. Priest. Cambridge (UK): Cambridge University, 2007
[40] Jaka Ortar, Re: Magnetogram 15-17.3.2015. From: Jaka Ortar <jaka@ freeapproved.com>, To: Damir Dezeljin <damir.dezeljin@dezo.org>; cc: Rudi Čop rudi@artal.si. Thu, Mar 19, 2015 at 12:24 PM.
[41] Rudi Čop, Damir Deželjin, Transmission of Measuring Data from the Sinji vrh Geomagnetic Observatory. Proceeding of the XVth IAGA Workshop on Geomagnetc Obsrvatory Instruments, Data Acquisition, and Processing. Edited by: Pavel Hejda, Arnaud Chulliat, Manuel Catalan. Extended Abstract Volume. San Fernadno; Cadiz (Spain): Real Instituto y Observatorio de la Armada, June 4th – 14 th, 2012. *Boletion Roa*, 2013, **3** (13), 160-164.
[42] Damir Deželjin, Rudi Čop, Prenos merilnih podatkov iz geomagnetenga observatorija po obstoječem komunikacijskem omrežju. *Raziskave s področja geodezije in geofizike 2014*. Zbornik del. Urednik Miran Kuhar. Ljubljana: Fakulteta za gradbeništvo in geodezijo, 2015, 127-132.
[43] Nigel P. Cook. Microwave Principles and Systems. New Jersey (US): Prentice Hall, 1986.
[44] Rudi Čop, Spomenko Mihajlović, Ljiljana Cander. Magnetic Storms and their Influence on Navigation. *Pomorstvo*, 2008, **22** (1), 89-99.
[45] Bruno Zolesi, Ljiljana R. Cander. *Ionospheric Prediction and Forecasting.* Heidelberg (D): Springer, 2014.
[46] David P. Stern, A brief history of magnetospheric physics before the spaceflight era. *Reviews of Geophysics*, 1989, **2** (7), 103-114.

Rudi Čop je leta 2003 doktoriral na Fakulteti za pomorstvo in promet Portorož pri Univerzi v Ljubljani in naslednje leto še na Fakultetu elektrotehnike i računarstva pri Sveučilištu u Zagrebu. Dela na področju meritev, merilnih instrumentov in obdelave merilnih podatkov. Od leta 2014 pri Zavodu Terra Viva, Sv. Peter 115, Sečovlje, vodi izgradnjo geofizikalnega observatorija Sikuri.

Vdori v omrežje in prisluškovanje na fizični optični infrastrukturi

Boštjan Batagelj, Laboratorij za sevanje in optiko, Fakulteta za elektrotehniko, Univerza v Ljubljani

Povzetek — Ob začetku uvajanja optičnih komunikacij pred 40 leti se je kot ena od prednosti navajala tudi nezmožnost prisluškovanja prometu, kar je bilo zelo preprosto pri bakrenih električnih vodnikih. Da signalu, ki potuje po dielektričnem optičnemu vlaknu ni mogoče prisluškovati, že zdavnaj ne velja več. Vedno bolj občutljivi optični sprejemniki in dovršene tehnološke rešitve danes omogočajo vdore in prisluškovanje tudi signalom v svetlobnih vlaknih. Prispevek podaja pregled metod prisluškovanja na optični infrastrukturi, kjer poznamo tri možnosti vdora. Pri začasni prekinitvi optične zveze operater opazi kratko prekinitev prometa, ko oseba z namenom prisluškovanja namešča prisluškovalno opremo. Prisluškovanje je mogoče izvesti tudi z začasno ali trajno poškodbo optičnega vlakna, ko sicer ne pride do prekinitve telekomunikacijskega prometa, vendar lahko operater s pomočjo natančne meritve optične moči ali stalnim nadzorom slabljenja v vlaknu zazna nezaželen vdor. Tretja možnost zlorabe zasebnosti pa je prisluškovanje signalom nižjih valovnih dolžin na osnovi Rayleightovega sipanja, kjer je operater v skorajda brezupnem položaju. Poleg pregleda možnosti prisluškovanja bo članek podal tudi nekaj smernic za zaznavo nezakonitih vdorov v jedrnem in dostopovnem delu optičnega omrežja.

Ključne besede — varnost, optično vlakno, optične tehnologije

Abstract — Fiber-optic links are indispensable telecommunications systems for all modern communications networks where a variety of data are transmitted. Communications worldwide are increasingly transmitted solely through fiber-optic lines, rather than through satellites and radios, because the capacity of fiber optics is so much greater than other communications media or technologies. As communications using fiber optics increase, the potential for the illegal eavesdropping and stealing of confidential and commercially sensitive data is growing.

This paper focuses on practical methods for eavesdropping on an optical telecommunication infrastructure. In order to listen to fiber-optic transmissions a tap must be physically placed somewhere along the route. The possibilities for intercepting the optical signals being transmitted across a network are reviewed.

In order to understand the various methods used to intercept optical signals, it is important to first understand that an optical fiber contains a core, where light is transmitted, and cladding, which creates a boundary layer that allows the light to reflect inside of the core by a process of total internal reflection.

The eavesdropper has several ways to intercept the optical signal traveling through the fiber. Basically, all the various methods can be divided into the following main categories:

1) interruption of the optical line,

2) damage to the optical fiber,

3) noncontact methods.

More sophisticated methods need better optical detectors – photodiodes with the proper wavelength range, a high sensitivity and a low dark current.

In the first category the operator can perceive a short interruption to the optical line, when the eavesdropper is setting up the interception equipment. The communications equipment is usually able to detect such an interruption, but it is impossible to locate the attack. In this category of eavesdropping there are various optical splitting techniques, for example, Fiber Bragg Gratings. An optical splitter with a splitting ratio of a few percent can be applied as a Fused Biconical Taper or as Planar Lightwave Circuits.

The second category of eavesdropping is using permanent or temporary damage to the optical fiber such as fiber bending or V-groove cutting to access the optical signal. In this case there is no need for interruption, so this kind of attack can be detected only by precise optical power monitoring or an online inspection of the fiber attenuation. The required bend radius depends on the type of optical fiber.

When the last category is used, the operator is helpless, since the eavesdropper is using evanescent coupling or optical scattering. Those phenomena occur all the time for reasons of optical fiber loss. This category of attack is only possible to detect and to battle against with advanced transmission techniques. In particular, optical Rayleigh scattering is wavelength dependent, so it is more suitable for lower wavelengths.

Nevertheless, all the various methods for eavesdropping on an optical fiber are more effective at the beginning of the optical line, because the transmitted optical power is decreasing with distance, so the portion of tapped power is lower.

– **Keywords —** security, optical fiber, optical technologies

I. UVOD

Optične zveze so nepogrešljive v vseh modernih komunikacijskih omrežij, po katerih se prenašajo najrazličnejši podatki. Zaradi vedno večje potrebe po pasovni širini [1], so optična vlakna s praktično neizmerno pasovno širino v vedno pogostejši uporabi za prenosni medij. Z naraščanjem uporabe optičnega vlakna v komunikacijske namene, se povečuje tudi možnost za nezakonito prisluškovanje in krajo zaupnih in poslovno občutljivih podatkov. [2].

Če želimo razumeti različne metode za prisluškovanje, je najprej potrebno razumeti zgradbo in delovanje optičnega vlakna [3]. Telekomunikacijsko optično vlakno je izdelano iz čistega kremenovega stekla in oblikovano v svetlovod okroglega preseka s premerom 125 μm. Stekleni svetlovod tvorita jedro, po katerem potuje svetlobni signal, in obloga, ki ima nižji lomni količnik od jedra, kar omogoča ujetost svetlobe v jedru. Osnova delovanja vseh dielektričnih valovodov je popolni odboj valovanja na meji dveh dielektrikov.

Ker so optična vlakna dielektrična, so odporna na elektromagnetne motnje. Zmotno je prepričanje, da je dielektrično optično vlakno, ki ga lahko polagamo praktično kjerkoli in ne povzroča nikakršnih problemov glede elektromagnetne kompatibilnosti, samo po sebi imuno na prisluškovanje. V samih začetkih optičnih komunikacij je res veljalo, da se signalom na optičnem vlaknu ne da prisluškovati, vendar je to veljalo samo zato, ker prisluškovanja ni bilo mogoče izvesti z do takrat razvitimi tehnikami prisluškovanja na bakrenih vodnikih. Danes so tehnike prisluškovanja na optičnih vlaknih že dobro razvite.

Glede na tehnično izvedbo prisluškovalne metode delimo v tri osnovne skupine [4]:

1. skupino sestavljajo metode, kjer je potrebo optično zvezo predhodno prekiniti;
2. skupino predstavljajo metode, kjer se trajno ali začasno poškoduje optično vlakno;
3. skupino predstavljajo metode, pri katerih ni potreben nikakršen poseg v optično vlakno.

Tovrstno razvrščanje metod temelji na možnostih operaterja za ugotavljanje napada na optično omrežje. Prvo skupino prisluškovalnih metod je mogoče zaznati kot krajšo prekinitev ob montaži prisluškovalne naprave in jo lahko zazna že sama komunikacijska terminalna oprema.

Pri drugi skupini prisluškovalnih metod ne pride do prekinitve optičnega signala, temveč se del le-tega odcepi na prisluškovalno napravo. Operater lahko zazna tovrstni napad s natančnim nadzorom moči prenesenega signala ali s stalnim nadzorom slabljenja optične zveze. V primerih, ko iz optične zveze poberemo manj kot 0,04 dB (~1%) moči prenesenega signala, kar je za prisluškovanje dovolj, uporabnikova komunikacijska oprema zaradi izredno majhnega padca moči zveze praktično ne more odkriti prisluškovanja.

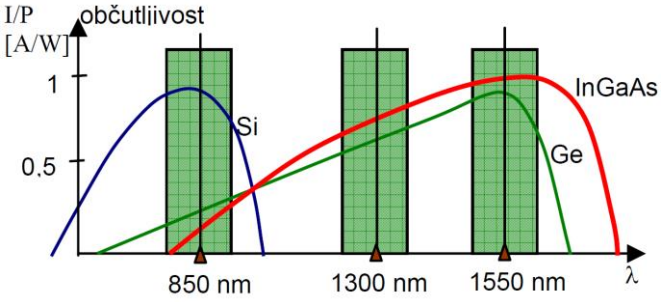
Pri zadnji skupini metod, ki so tudi najtežje izvedljive se ne posega v delovanje optičnega vlakna temveč se koristi signale, ki prihajajo iz vlakna med prenosom signala. Zadnjo skupino napadov je nemogoče zaznati in se proti njej lahko borimo samo z izpopolnjenimi tehnikami prenosa.

Vse naštete prisluškovalne metode potrebujejo primeren svetlobni detektor. Ustreznost detektorja je odvisna od valovne dolžine in njegove občutljivosti, ki je direktno povezana z močjo prisluškovalnega signala. Potreba po večji občutljivosti detektorja narašča z zahtevnostjo prisluškovalne metode, ki je premosorazmerna s težavnostjo odkrivanja prisluškovalca. Bolj občutljiv detektor omogoča osebi, ki izvaja vdor, uporabo manjše moči optičnega signala, kar oteži operaterju odkriti napad in določiti njegovo lokacijo.

V splošnem je edini praktično uporaben detektor za pretvorbo svetlobnih komunikacijskih signalov v električne polprevodniška fotodioda. Pri vseh ostalih pretvornikih imamo počasen odziv ali majhno občutljivost ali slabo razmerje signal/šum. Vse fotodiode za optične komunikacije se uporabljajo v zapornem režimu delovanja, kar pomeni, da imajo razmeroma debelo zaporno plast, kar omogoča visok kvantni izkoristek, običajno preko 80%.

Polprevodniške fotodiode so narejene iz polprevodnikov, kot so silicij, germanij in elementov III. in IV. skupine periodičnega sistema. Za delovanje v področju valovnih dolžin od 1300 nm do 1550 nm ne moremo več uporabljati silicijevih fotodiod, v poštev pridejo le germanijeve fotodiode in fotodiode iz sestavljenih polprevodnikov (slika 1).

Od fotodiode namenjene prisluškovanju je poleg ustreznega valovnodolžinskega področja zaželena tudi čim večja občutljivost in čim manjši temni tok. Temni tok je poglavitni vir šuma pri zelo nizkih osvetlitvah. To je tok, ki teče skozi popolnoma zatemnjeno fotodiodo, ob prisotnosti zaporne napetosti. Ker je zelo temperaturno odvisen, so tovrstni detektorji ustrezno hlajeni na kriogenske temperature.



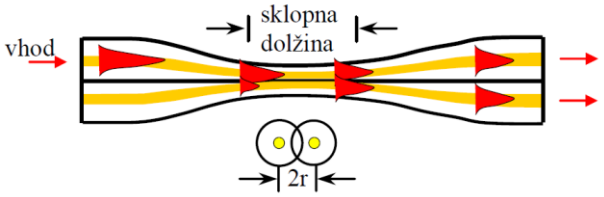
Slika 1: Odzivnost različnih polprevodniških fotodiod

V primeru vdora v optično zvezo občutljiva fotodioda pretvori svetlobni signal v električnega in uporabi dodatno elektroniko za ojačanje podatkovnega signala. S tem je signal pripravljen za analizo in ovrednotenje z ustrezno programsko opremo.

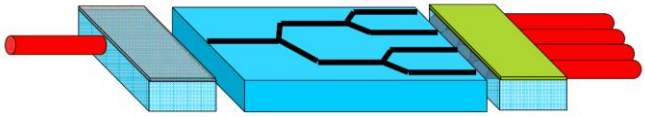
II. PRISLUŠKOVANJE S PREDHODNO PREKINITVIJO OPTIČNE ZVEZE

Najenostavnejša metoda prisluškovanja signala v optičnem vlaknu je osnovana na prekinitvi vlakenske zveze in umestitvi primerne optične naprave za prisluškovanje. Med nameščanjem prisluškovalne naprave pride do prekinitve telekomunikacijske zveze. V kolikor je prekinitev zveze kratka, jo operater smatra kot motnjo in prometni pretok potuje neomejeno, ne da bi operater posumil, da je prišlo do vdora.

Najenostavnejši prisluškovalni element, ki ga lahko vstavimo v optično zvezo je pasivni optični razcepnik [5]. V pasivnem optičnem dostopovnem omrežju se tovrstne naprave uporabljajo za deljenje signala iz centrale na mnogo uporabnikov [6]. Za vsak optični razcepnik so predvsem pomembni trije parametri. Prvi je delitveno razmerje, ki je največkrat 50:50, vendar se v praksi srečujejo tudi drugačna razmerja predvsem v slučajih, ko želimo izvajati sam nadzor omrežja in odcepiti zelo majhen del signala (kakšen odstotek). Ostala pomembna prametra sta vstavitveno slabljenje, ki podaja koliko svetlobnega signala se izgubi na napravi sami; in valovno dolžinsko oziroma frekvenčno področje delovanja. Tipično vstavitveno slabljenje znaša okrog 0,5 dB, kar pomeni, da se pri razcepniku 50:50 signal oslabi za 3,5 dB. Če je delitveno razmerje ustrezno manjše, je manjša tudi vstavitvena oslabitev operaterjevega signala, vendar v nobenem primeru ne pade pod 0,5 dB. Pri vrednotenju razcepnikov po frekvenčnem področju delovanja poznamo razcepnike, ki delujejo samo znotraj enega ali več spektralnih oken. Osnovni spojni strukturi sta Y-spoj ali 1×2 spojnik (naprava s tremi priključki) in X-spoj ali 2×2 spojnik (naprava s štirimi priključki). Spojni strukturi sta lahko narejeni z varjenimi enorodovnimi ali mnogorodovnimi vlakni (angl. Fused Biconical Taper – FBT) ali s pomočjo planarnih vezji (angl. Planar Lightwave Circuits – PLC), kot prikazujeta sliki 2 in 3.

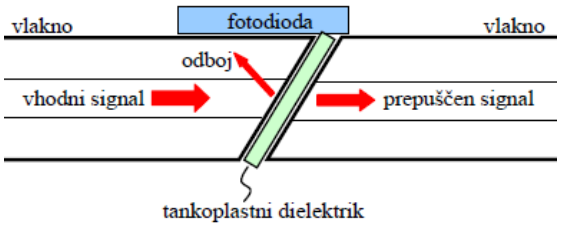


Slika 2: Zgradba varjenega vlakenskega razcepnika



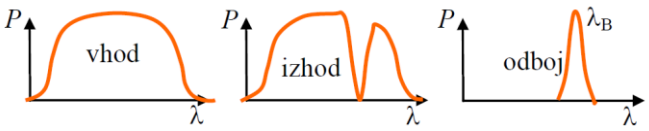
Slika 3: Zgradba planarnega optičnega vezja kot razcepnika

V samo prekinjeno zvezo se lahko vstavi tudi prisluškovalni element, ki vsebuje polprepustno zrcalo [7]. Signal, ki potuje po optičnem vlaknu, se prestreže s polprepustnim zrcalom, kot prikazuje slika 4. Polprepustno zrcalo s svojimi lastnostmi omogoča 95% prepustitev signala, 5% pa odbije proti fotodiodi pod kotom 20º. Element je bil v osnovi razvit za nadzor WDM sistema, njegovo vstavitveno slabljenje pa je manjše od 1 dB.



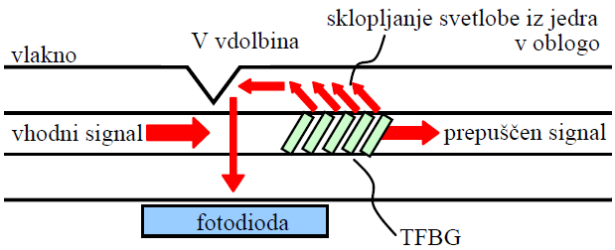
Slika 4: Polprepustno zrcalo v vlaknu

Poleg zrcala je za prisluškovanje možna tudi uporaba Braggove uklonske mrežice (angl. Fiber Bragg Gratings – FBG). Ker je uklonska mrežica frekvenčno selektiven element, omogoča prisluškovanje signalom na točno določeni izbrani valovni dolžini, kot je prikazano na sliki 5.



Slika 5: Spektralni odziv Braggove uklonske mrežice

Z namenom izločitve odbitega signala iz vlakna se za prisluškovanje uporabi poševna optična Bragova uklonska mrežica (angl. Tilted Fiber Bragg Grating – TFBG) z naklonom približno 3 stopinje (slika 6) [8]. Svetloba ki potuje po vlaknu je deležna dveh odbojev. Prvi je odboj iz jedra na oblogo, kar je učinek TFBG. Drugi, popolni odboj se zgodi na V-utoru vrezanemu v oblogo optičnega plašča [9].

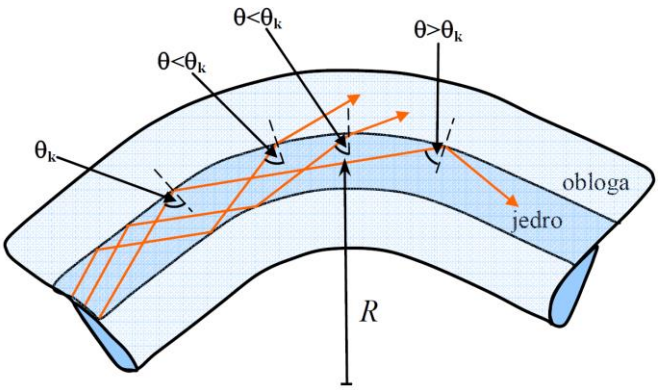


Slika 6: Poševna Braggova uklonska mrežica in V utor za izločitev optičnega signala

III. PRISLUŠKOVANJE S POŠKODOVANJEM OPTIČNEGA VLAKNA

Metode prisluškovanja optičnemu signalu z začasnimi ali trajnimi poškodbami je mogoče izvesti ne da bi predhodno prekinili optično vlakno oziroma podatkovni pretok. Kablu je potrebno predhodno le odstraniti sekundarno in primarno izolacijo in ga ustrezno deformirati. Začasna deformacija je v primeru, ko vlakno zgolj ukrivimo. Trajna deformacija, pa ko ga spoliramo, vanj vrežemo V utor ali v jedru ustvarimo periodično strukturo.

Svetlobno vlakno je optični valovod, pri katerem se na krivinah pojavi izhajanje svetlobe, kar za prenašani signal pomeni slabljenje [10]. Zaradi izredno položnega kota pri popolnem odboju na meji med jedrom in oblogo vlakna se lahko zgodi, da po upognitvi vlakna za krivinski polmer R niso več izpolnjeni pogoji popolnega notranjega odboja na zunanji krivini vlakna, kot je prikazano na sliki 7. Svetlobni žarek, ki pride do krivine optičnega vlakna, ima vpadni kot manjši od kota za popolni odboj θ_k, kar pomeni, da uide v oblogo in je za prenos izgubljen. Žarki, ki vpadejo na krivino pod še ustrezajočim kotom ($\theta>\theta_k$), lahko obidejo ukrivljenost. To pomeni, da žarek uhaja iz jedra, vlakno seva v okolico, val v vlaknu pa se oslabi.

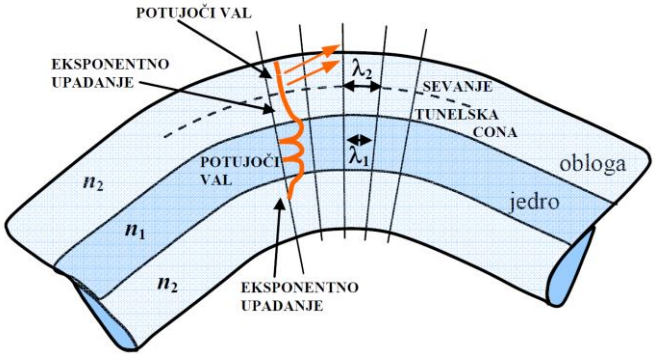


Slika 7: Prikaz krivinskega slabljenja

Pojav uhajanja dela optične moči na krivinah je še posebno izrazit pri šibkolomnih valovodih, kjer je razlika med lomnim količnikom jedra n_1 in obloge n_2 razmeroma majhna. Pri komunikacijskih vlaknih je vsekakor pomemben minimalni krivinski polmer, pri katerem bo svetloba začela uhajati iz optičnega vlakna. Krivinsko slabljenje je odvisno od izvedbe dielektričnega valovoda, pri čemer pomembno vlogo igra debelina obloge in razlika med lomnima količnikoma.

Pojav natančneje pojasnimo s pomočjo valovne optike. Na krivinah svetlobnega valovoda valovne fronte niso več vzporedne, pač pa se pahljačasto odpirajo. Razmak valovnih front na notranji strani krivine se zmanjša, na zunanji strani krivine pa poveča. Ko postane razmak med valovnimi frontami večji od valovne dolžine v oblogi z lomnim količnikom n_2, eksponentno upadajoče elektromagnetno polje preide v potujoče valovanje (slika 8).

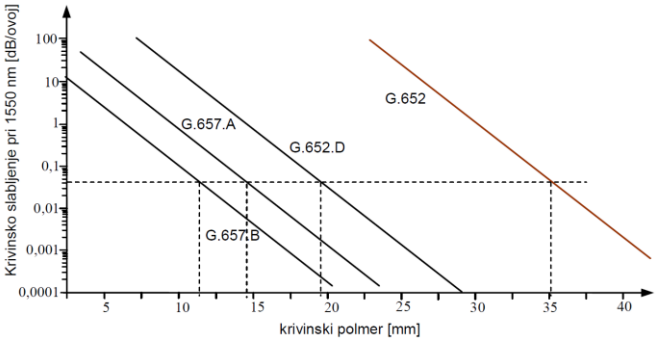
Za standardno enorodovno optično vlakno G.652, ITU-T standard zahteva, da slabljenje ne presega 1 dB moči signala pri stotih ovojih na osi polmera 37,5 mm [11]. Krivinska slabljenja standardnega vlakna na krivini 2,5 cm so v velikostnem razredu 0,01 dB, kar je že opazno s komercialnim terenskim merilnim instrumentarijem. V novejšem izpopolnjenem standardu G.652.D, kjer je vlakno optimizirano za nizkek PMD in OH slabljenje, je krivinsko slabljenje ustrezno nižje.



Slika 8: Uhajanje (tuneliranje) dela moči valovanja na krivini dielektričnega valovoda

Pri inštalacijah vlakna na dostopovnih omrežjih je nizko krivinsko slabljenje pomemben parameter, zato so pri ITU-T osnovali standard G.657 za vlakno z nizkim krivinskim slabljenjem. Podstandard G.657.A se navezuje na vlakno, ki je kompatibilno z vlaknom tipa G.652, in ju lahko medseboj spajamo. Vlakno G.657.B je namenjeno uporabi v zgradbah in ne izraža potrebe po kompatibilnosti s standardom G.652. G.657.B je vlakno z majhnim premerom jedra (do 6,3 μm) in stopničastim lomnim likom.

Slika 9 prikazuje odvisnost slabljenja od krivinskega radia za standardna enorodovna vlakna G.652, G.652.D in vlakni z izboljšanimi lastnostmi krivljenja G.657. ITU-T standard za optično vlakno G.657.A narekuje slabljenje pod 0,75 dB pri 10 mm polmeru enega ovoja. Za G.657.B je ta zahteva še ostrejša in znaša 0,5 dB na 7,5 mm polmeru enega ovoja.

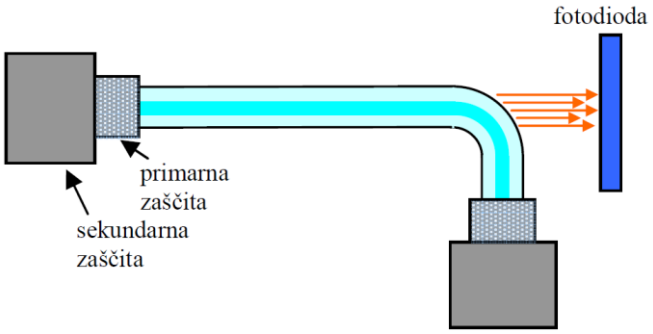


Slika 9: Krivinsko slabljenje pri 1550 nm za različne tipe optičnega vlakna v odvisnosti od krivinskega polmera

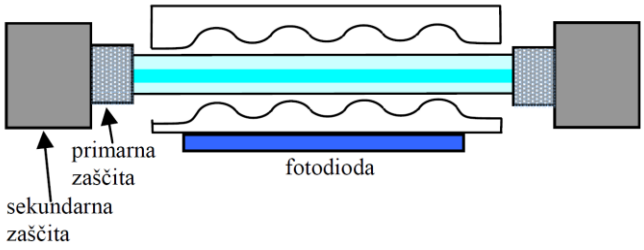
Za prisluškovanje v optičnih zvezah zadostuje že 1% odcepljenega signala, kar je približno 0,04 dB. Iz slike 9 lahko razberemo, da je za namene prisluškovanja potrebno ustvariti krivinski polmer 35 mm za vlakno G.652, 19 mm za vlakno G.652.D, 14 mm za vlakno G.657.A in 11 mm za vlakno G.657.B. Proizvajalci optičnih vlaken lahko za nekaj razredov prekašajo zahteve zapisane v standardu, tako da je na trgu mogoče zaslediti vlakna z nižjim slabljenjem na krivinah, kot zahteva standard.

Vlakna z nižjim krivinskim slabljenjem zahtevajo večjo ukrivljenost z namenom prejemanja zadostne optične moči. Z dovolj majhno krivino je še vedno mogoče prejeti dovolj optične moči za izvedbo prisluškovanja. Tehnologija vlaken, ki imajo nižje krivinske izgube torej ne onemogoča prisluškovanja. Možnosti za prisluškovanje ne bi bilo v primeru, če bi se pri ukrivljanju vlakno pretrgalo.

Svetlobo, ki tunelira iz ukrivljenega vlakna, je najprimerneje takoj ujeti na polprevodniško fotodiodo. Krivljenje vlakna se lahko izvede na eni makro krivini ali več mikrokrivinah, kot prikazujeta sliki 10 in 11. Naprave, ki uporabljajo mikro krivine so namenjene ugotavljanju prisotnosti optičnega signala in smeri potovanja signala, ter se običajno uporabljajo pri vzdrževanju optičnega omrežja in manj za namene prisluškovanja.



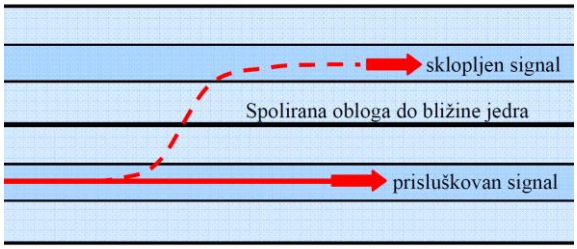
Slika 10: Prisluškovanje na osnovi makro krivine



Slika 11: Prisluškovanje na osnovi mikro krivin

Namesto na krivinah je svetlobo mogoče dobiti iz vlakna tudi s pomočjo sipanja na umetno ustvarjenih nezveznostih. [12] V ta namen se lahko vlakno greje ali obdeluje s CO_2 laserjem. V točki obdelave prihaja do dodatnega sipanja svetlobe, ki se jo ujame na fotodiodo.

Podobno kot v prejšnjem sklopu opisane metode optičnega razcepnika je mogoče signal pridobiti iz optičnega vlakna tudi, ko se optična zveza ne prekine. Pri tem se v sosednje vlakno sklaplja valovanje, ki se izgublja v oblogi optičnega vlakna, kot prikazuje slika 12. S poliranjem obloge skoraj do jedra vlakna, ki povezuje centralo in uporabnika in vlakna, na katerega se sklaplja signal, je mogoče pridobiti dovolj svetlobne moči za izvedbo prisluškovanja.

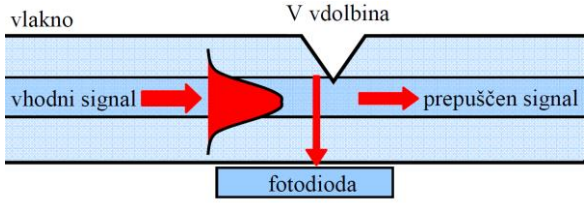


Slika 12: Prisluškovanje na osnovi približevanja jeder

Signal je mogoče izločiti iz optičnega vlakna tudi s pomočjo zareze v oblogo optičnega vlakna. Zareza mora imeti obliko črke V, pri čemer mora biti kot med smerjo razširjanja signala in ploskvijo V izreza večji od kota potrebnega za popolni odboj. Ko je ta pogoj izpolnjen, se del signala, ki sega v oblogo, odbije od V zareze in izhaja iz vlakna, kot prikazuje slika 13.

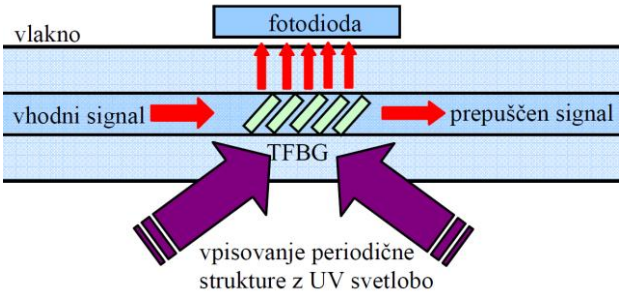
Metoda zahteva natančno izdelan izrez v vlakno in celo poliranje samega izreza. Za izvedbo je potrebna zelo precizna oprema in postopek za namestitev tovrstne prisluškovalne

naprave zahteva dovolj časa. Vdor je težko odkriti, ker natančno izdelana naprava odvzema majhen del optične moči. Metoda zahteva rezanje V utora v optično vlakno, ki se pri tem lahko pretrga, kar povečuje možnost odkritja lokacije vdora.



Slika 13: Svetloba odbita od izrezanega V-utora

Najbolj napredna tehnika v tej skupini prisluškovalnih metod in tudi najtežja za odkrivanje je izdelava Braggove uklonske mrežice v samem optičnem vlaknu. Proces izdelave uklonske mrežice zahteva zunanji UV laser in pripadajoče fazne maske. Uklonska mrežica mora biti izdelana pod kotom, da odbija signal iz vlakna, kot prikazuje slika 14. Ker je Braggova mrežica frekvenčno selektivna, je na ta način izsejana zgolj določena valovna dolžina.



Slika 14: Sipanje optičnega signal na poševni vlakenski Braggovi uklonski mrežici

IV. PRISLUŠKOVANJE NA OSNOVI RAYLEIGHTOVEGA SIPANJA

V dielektričnih valovodih obstaja elektromagnetno polje v celotnem prostoru valovoda. V sredici valovoda z višjim lomnim količnikom n_1 ima vodeni val obliko stojnega vala, v oblogi valovoda z nižjim lomnim količnikom n_2 pa ima polje vodenega vala obliko eksponentno upadajočega polja.

Elektromagnetno polje dielektričnega valovoda se torej vedno razteza v neskončnost in v matematičnem pogledu ne more biti zaključeno. V vseh praktičnih dielektričnih valovodih izberemo dovolj debelo oblogo n_2 in dovolj hitro eksponentno upadanje polja, da je polje na zunanji meji obloge zanemarljivo majhno. Svetlobna moč, ki uide iz obloge, je sicer izgubljena, vendar je pri primernem načrtovanju dielektričnega valovoda ta moč zanemarljivo majhna.

Optični signal, ki se širi po vlaknu prispe na konec zveze oslabljen. Njegova oslabitev je odvisna od faktorja slabljenja, ki ima valovnodolžinsko odvisnost in pri valovni dolžini 1550 nm znaša približno 0,2 dB/km. Glavni vir slabljenja signala v optičnem vlaknu je Rayleighovo sipanje. Le-to razprši svetlobo, ki potem lahko izhaja iz vlakna. Za razliko od loma in odboja, kjer se svetlobno valovanje po pojavu odbije samo v eno smer, se pri sipanju razprši svetloba v vse smeri. Sipanje svetlobe se vrši na naključno porazdeljenih delcih (molekulah) snovi, ki je v našem primeru steklo.

Selektivno sipanje ali Rayleighovo sipanje se pojavi, ko imajo delci snovi lastnost, da bolj učinkovito sipajo svetlobo izbrane valovne dolžine. Običajno je tako, da se svetloba krajših valovnih dolžin bolj sipa kot svetloba daljših valovnih dolžin. Z naraščanjem valovne dolžine Rayleighovo slabljenje optičnega vlakna pada s četrto potenco.

Z naraščanjem valovne dolžine slabljenje optičnega vlakna pada in teoretično lahko pride do izredno nizkih slabljenj pri visokih valovnih dolžinah. V praksi pa se pri večjih valovnih dolžinah pojavi absorpcija svetlobe v steklu.

Minimalno slabljenje optičnega vlakna nastopi pri valovni dolžini 1550 nm in to je tudi razlog za nastanek tretjega spektralnega okna v optičnih komunikacijah.

Na osnovi Rayleighovega sipanja je mogoče izvesti prisluškovanje, ne da bi kakorkoli fizično posegali v vlakno in proizvajali dodatno izhajanje svetlobe. Iz vlakna že sam po sebi izhaja optični signal zaradi sipanja. Ta signal je potrebno le ujeti na fotodiodo in ga ustrezno ojačiti. S pomočjo Rayleighovega sipanja je mogoče priti do optičnega signala neopazno. Tovrstnega prisluškovanja ne bi bilo mogoče razkriti, kajti na prenašanem signalu ne nastane nobena dodatna motnja in sistem navzven ne prikazuje kakršnekoli dodatne izgube signala.

Prisluškovalna naprava na osnovi Rayleighovega sipanja je narejena iz foto detektorja in zrcala na drugi strani optičnega vlakna. Za fotodetektor je predvidena polprevodniška InGaAs fotodioda. V primeru 5 mm detektorja je mogoče pri 1550 nm pridobiti dovolj signala za prisluškovanje. Jakost Rayleighega sipanja je odvisna od valovne dolžine svetlobnega signala. S povečanjem valovne dolžine jakost sipanja postane občutno manjša.

V primeru enorodovnega vlakna z NA=0,1, se le zanemarljiv del (približno 0,2%) sipane svetlobe ujame nazaj v jedro vlakna, vsa ostala svetloba se sipa v stekleno oblogo. Iz optičnega vlakna pride samo 45% izsevane svetlobe, saj se preostala svetloba ujame v plašč, ker zadosti kotu popolnega odboja na meji obloga–zrak. Torej lahko iz vlakna s slabenjem 0,4 dB/km pričakujemo na dolžini enega centimetra približno -63 dB odcepljenega signala, ki ga je s pomočjo zrcala mogoče ujeti na fotodiodo.

V. ZAKLJUČEK

Prispevek nazorno prikazuje možnosti za prisluškovanje telekomunikacijskemu prometu, ki ga prenašamo po optičnih vlaknih. Večina naprednih uporabljenih metod za prisluškovanje ne povzroči prekinitve zveze. Do signala je mogoče dostopati že z manjšimi deformacijami vlakna, kot je na primer krivljenje. Sodobna vlakna so bolj odporna na krivinske izgube vendar to ne onemogoča prisluškovanja, ki ga je z dovolj majhnimi še vedno možno izvesti.

Za zmanjšanje možnosti prisluškovanja je potrebno pri izgradnji transportnih in dostopovnih omrežij z optičnim vlaknom načrtovati tudi ustrezno zaščitno metodo. Priporočljiv je stalni nadzor slabljenja zveze z naprednimi OTDR tehnikami [13], uporaba zahtevnejših modulacijskih formatov ali/in elektronsko šifriranje podatkov.

Tako rekoč nezlomljivim zaščitnim tehnikam elektronskega šifriranja, ki varujejo naše podatke na višjem nivoju omrežja, zdaj prihaja v dopolnitev kvantno šifriranje [14], ki omogoča tudi teoretsko nezlomljivo varovanje podatkov na samem fizičnem nivoju telekomunikacijskih povezav s pomočjo optičnega vlakna. Medtem ko klasično šifriranje uporablja različne matematične metode za zaščito

sporočila pred prisluškovanjem, kvantno šifriranje temelji na uporabi zakonov kvantne fizike za doseganje absolutne varnosti prenosa podatkov.

ZAHVALE

Delo predstavljeno v tem prispevku je nastalo s pomočjo Javne agencije za raziskovalno dejavnost Republike Slovenije (ARRS) v okviru programa "Algoritmi in optimizacijski postopki v telekomunikacijah". Za pomoč pri pregledu opreme in za koristne nasvete se avtor zahvaljuje podjetjema InLambda BDT d.o.o. in Xenya, d.o.o.

LITERATURA

[1] Boštjan Batagelj, Vijay Janyani, Sašo Tomažič, Research challenges in optical communications towards 2020 and beyond. Informacije MIDEM, letn. 44, št. 3, str. 177-184, 2014. http://www.midem-drustvo.si/Journal%20papers/MIDEM_44(2014)3p177.pdf
[2] A. Teixeira, A. Vieira, J. Andrade, A. Quinta, M. Lima, R. Nogueira, P. André, G. Tosi Beleffi, Security Issues in Optical Networks Physical Layer, ICTON 2008.
[3] M. Vidmar, Optical-fiber communications: components and systems. Inf. MIDEM, letn. 31, št. 4, str. 246-251, 2001
[4] Marcus Moser, Eavesdropping on Light, Crypto Magazine, št. 2, str. 14–15, 2007
[5] Arun K. Agarwal, Review of optical fiber couplers, Fiber and Integrated Optics, Vol. 6, Issue 1, , pp 27–53, 1987
[6] Boštjan Batagelj. Pasivno optično dostopovno omrežje s časovnim razvrščanjem. 1. izd. Ljubljana: Založba FE in FRI, 2011. 124. str.
[7] H. Kuwahara, S. Saito, A Semi-Transparent Mirror-Type Directional Coupler for Optical Fiber Applications, IEEE Transactions on Microwave Theory and Techniques, Volume 23, Issue 1, pp. 179–180, Jan 1975
[8] Seihyoung Lee, Shinyoung Yoon, Jong Jin Lee, Chong Hee Yu and Hyun Seo Kang, Optical signal is coupled out using fiber grating, Optoelectronics & Optical Communications, 22 May 2007, SPIE Newsroom
[9] Seihyoung Lee, Shinyoung Yoon, Jong Jin Lee, Chong Hee Yu, and Hyun Seo Kang, Experimental and theoretical characterization of optical signal out-coupling through V-grooved optical fiber cladding, Opt. Eng., Vol. 45, December 2006, 99
[10] R.W. Smink, B.P. de Hon and A.G. Tijhuis, Bend-Induced Loss in Single-Mode Fibers, Proceedings Symposium IEEE/LEOS Benelux Chapter, 2005, Mons, pp.281 – 284
[11] Characteristics of a single-mode optical fibre cable ITU-T. G.652 Recomendation
[12] D. Scott Shenk and Leonard G. Cohenm, Fiber-optic Tapping Via Induced Scattering, Journal of Lightwave Technology. Vol. 7. No. 1O. October 1989, p.p. 1556 – 1558
[13] A. Champavere, New OTDR measurement and monitoring techniques, Optical Fiber Communications Conference and Exhibition (OFC), March 2014
[14] Jurij Tratnik, Boštjan Batagelj. Predstavitev ideje kvantnega šifriranja in pregled osnovnih tehnik kvantnega razdeljevanja ključa. Elektrotehniški vestnik, 2008, letn. 75, št. 5, str. 257-263

Boštjan Batagelj je docent na Fakulteti za elektrotehniko Univerze v Ljubljani, kjer predava predmete satelitske komunikacije in navigacija, optične komunikacije in radijske komunikacije. Raziskovalno delo opravlja v Laboratoriju za sevanje in optiko, kjer se med drugim ukvarja s fizičnim nivojem prenosnih in dostopovnih telekomunikacijskih omrežjih zasnovanih na radijski in optični tehnologiji. Je avtor več kot 300 člankov, osmih patentnih prijav in sodeluje v domačih ter mednarodnih raziskovalnih projektih s področja optičnih in radijskih komunikacij.

Cybersecurity today and tomorrow: the future of IT Security in Critical Infrastructure

Johan L. Eliasson, Stefan Chevul and Martin Nordqvist, Advenica AB, Vienna, Austria

Abstract — Critical infrastructure has long been considered immune to the cyber attacks. Unfortunately, this complacency is misplaced cybersecurity has recently become an issue of legitimate combat. The shift to open standards such as Ethernet, TCP/IP and web technologies enables hackers take advantage of the control industry's ignorance.

This paper looks at the nature of the threats posed past and present, and offer strategies to keep critical infrastructure systems safe. The strategies are based on emerging technologies available today bridging the huge gap between critical infrastructure security research in academia and industrial practice.

Keywords — cybersecurity, cyber warfare, cyberattack, critical infrastructure

I. INTRODUCTION

According to the UK cabinet office [1], the internet-related market in the UK is estimated at £82 billion (almost €100 billion) a year, with British businesses earning £1 in every £5 from the Internet.

However, this greater digital openness, interconnection and dependency bring vulnerability. The UK National Security Strategy has categorized cyber attacks as a Tier One threat to national security, alongside international terrorism, with terrorists, rogue states and cyber criminals targeting computer systems in the UK.

93% of large corporations and 87% of small businesses reported a cyber breach in the past year. On average over 33,000 malicious emails are blocked at the Gateway to the Government Secure Intranet (GSI) every month.

With the cost for a cybersecurity breach estimated between £450,000 to £850,000 (over €1 million) for large businesses and £35,000 to £65,000 (nearly €80,000) for smaller ones, governments must look at new ways to protect businesses and critical infrastructure; and make their countries more resilient to cyber attacks and crime.

The general definition of cybersecurity is to put in place tools, policies, security concepts, security safeguards, guidelines, risk management, approaches, actions, training, best practices, assurance and technologies to protect the cyber environment and organization and the user's assets.

II. CYBER WARFARE

Cyber warfare can be used to conduct political, economic or military attacks. Cyber warfare can also be used to conduct espionage including industrial espionage, allowing a country to potentially gain access to another nation's secrets with little risk.

Attacks are becoming more frequent and are often attributed to Hackivists, politically motivated hackers whose attacks range from the annoying defacement of websites to full-scale attacks on a target country, as was the case in Estonia in 2007.

There is a debate as to whether these hacktivists are controlled by a nation state, or are simply a loose band of people on a cause. Much of the evidence points to the former. That nation states lie behind many of the attacks. One question that arises is whether the Estonia incident was an incidence of cyber warfare.

Scott D Applegate from the US army argues that there is no legal definition of cyber warfare and there is unlikely to be one in the near future. He further argues that cyber warfare provides attackers with plausible deniability, since Internet attacks are difficult to track to a single origin.

III. CRITICAL INFRASTRUCTURE AT RISK

What Applegate describes as cyber militia, a confederation of hacktivists funded by a nation-state who perpetrate cyberattacks, can achieve their political objectives without adhering to the Law of Armed Conflict. The UN defines this as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations."

While many militaries use computers as a weapon system, it's debatable whether using computer systems to attack a country can be deemed as using armed force. Under the Law of Armed Conflict, armed forces must distinguish between military and civilian targets. However, distinguishing targets in cyberspace is difficult, as people can only identify the majority of systems by their Internet protocol addresses and domain names.

Cyberattackers targeting a nation-state's information infrastructure may well cause collateral damage to civilian systems and critical infrastructure.

Appelgate also points out that the greatest concern to most security analysts is that critical infrastructure is particularly vulnerable to cyber warfare.

While there is no record of anyone ever having died due to a cyber attack or because of a computer being hacked, vulnerabilities associated with critical infrastructure, especially Supervisory Control and Data Acquisition (SCADA) systems, poses a serious threat.

SCADA systems are networked computers that automate the control of infrastructure systems such as the electrical grid, sewage systems, utilities and traffic control systems.

An example of an attack on a SCADA system is when a disgruntled former employee hacked into the sewage system in Queensland, Australia and released an estimated million liters of raw sewage into rivers and coastal waters. The attacker attempted to hack into the system 44 times from a

remote location without being detected until he finally succeeded.

IV. 1982 - THE FIRST INCIDENT

Since as far back as 1982 there have been several cases of cyberattacks where nation states are suspected of being the instigators.

In 1982 the CIA used a so called logic bomb to blow up a Siberian gas pipeline. The Trans-Siberian Pipeline required an advanced SCADA system. The pipeline used plans for a sophisticated control system and its software that had been stolen from a Canadian firm by the KGB. The CIA allegedly had the company insert a logic bomb in the program for sabotage purposes. The result was a violent explosion with the power of three kilotons of TNT. The attack had an enormous economic and psychological effect on the Soviet Union and is credited with helping end the Cold War.

On April 26, 2007, the Baltic State of Estonia experienced the first wave of Distributed Denial-of-Service (DDoS) attacks. These cyberattacks were launched as a protest against the Estonian government's removal of the Bronze Soldier monument in Tallinn, a Soviet war monument erected in 1947.

The attacks targeted prominent government websites along with the websites of banks, universities, and Estonian newspapers. After three weeks, the attacks ceased as suddenly as they had begun, but not before the Estonian government undertook measures to block all international web traffic, effectively shutting off the "most wired country in Europe" from the rest of the world.

The cyber attack on Estonia led NATO to establish the Cooperative Cyber Defense Center of Excellence in 2008, focusing on coordinating cyber defense and establishing policies for aiding allies during cyber attacks.

The importance of these cyberattacks lies not in their size or scope, but rather in the precedent they created for future cyber conflicts. Since then, cyberattacks have become a proven political weapon as a way of intimidating enemies, silencing them, and potentially controlling their infrastructure.

On 6 September 2007, Israeli aircraft carried out a bombing raid on a Syrian nuclear reactor being constructed by North Korean technicians. Codenamed Operation Orchard, the Israeli military reportedly used technology similar to the USA's Suter airborne network to feed enemy radar with false targets and directly manipulate enemy sensors. This allowed Israeli jets to pass through undetected and carry out their mission. Some sources also maintained that the Israeli military had deactivated the Syrian air defense network using a secret built-in switch.

V. THE LARGEST CYBER ATTACK TO DATE

In June 2010, a security company identified the malware that became known as Stuxnet. It is designed to infect SCADA systems targeting the Iranian nuclear program.

Stuxnet is a sophisticated program that disguises the damage it is wreaking from operators and overseers, until it is too late to reverse. Evidence suggests that Stuxnet was first created in 2005.

Stuxnet contained two different attack routines; the smaller and simpler attack routine that changes the speeds of centrifuge rotors. The other routine attempted to over-pressurize centrifuges, causing solidification of process gas. This would have resulted in simultaneous destruction of hundreds of centrifuges per infected controller. However it seems the attackers took care to avoid catastrophic damage, which they could have potentially caused.

Stuxnet is thought to have inflicted substantial damage to the Iranian nuclear centrifuges, putting the program off track for several years. While the attack was specific, the tactics and technology used are generic and can be used against other targets. Stuxnet is seen as an opening act of cyberwarfare in today's IT society.

Duqu, often called "Son of Stuxnet", was found on a number of corporate computer systems in Europe in 2011. Based on the Stuxnet source code, Duqu is used as a backdoor to allow attackers to remotely access compromised systems to siphon off sensitive information and gather intelligence, potentially for use in future attacks.

Duqu disguises itself as a device driver that loads when the system boots. Basically, Duqu can steal anything from a targeted system, including passwords, take desktop screenshots, and steal documents. This malware runs on an infected system for 36 days before deleting itself, staying under the radar.

Probably the most complex malware ever discovered, Flame targeted several Middle-eastern countries in 2012, including Iran, Israel, Sudan, Syria, Lebanon, Saudi Arabia and Egypt.

Dedicated to stealing data, this virus turned computer microphones into listening devices, take screenshots, copying instant message chats and even keyboard strokes.

Like Stuxnet and Duqu, Flame was probably commissioned by a nation state and seemed to primarily target Iran.

VI. HUMANS EXPLOIT SYSTEM WEAKNESSES

Many examples of breaches of data security are human, where people exploit weaknesses in a given system to steal sensitive information. Two recent examples that gained world attention are Bradley Manning and Edward Snowden.

Private Bradley Manning downloaded thousands of classified documents from military servers and passed them on to WikiLeaks. As an intelligence analyst in the US Army, Pte Manning was given access to a large amount of highly sensitive information which he saved on a CD-R which he labeled "Lady Gaga". According to an interview with the magazine Wired, Manning confessed to former hacker Adrian Lamo, saying that he encountered, "Weak servers, weak logging, weak physical security, weak counter-intelligence, and inattentive signal analysis… a perfect storm."

Former employee of the Central Intelligence Agency (CIA) and former contractor for the National Security Agency (NSA), Snowden worked as a systems administrator for private contractor Booz Allen. He came to international attention while working as a systems administrator, when he downloaded thousands of classified documents on to thumb drives and disclosed them to several media outlets.

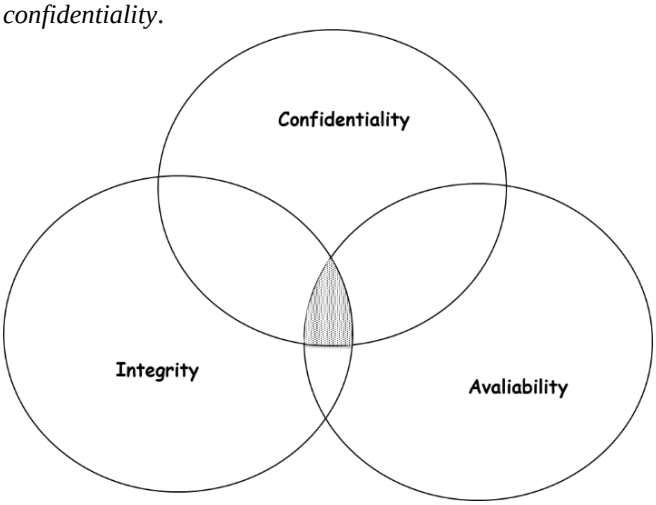
The leaked documents revealed operational details of global surveillance programs run by the NSA and the other Five Eyes governments of the United Kingdom, Australia, Canada, and New Zealand, with the cooperation of a number of businesses and European governments.

The release of classified material was called the most significant leak in US history by Pentagon Papers leaker Daniel Ellsberg.

A series of exposés beginning June 5, 2013, revealed Internet surveillance programs such as PRISM, MUSCULAR, XKeyscore and Tempora, as well as the bulk collection of US and European telephone metadata. The reports were based on documents Snowden leaked to The Guardian and The Washington Post.

VII. PREVENTING CYBER ATTACKS

By taking precautions in three key areas it is possible to reduce cyber attacks to a minimum, keeping critical systems secure. These areas are: *availability*, *integrity*, and *confidentiality*.



Picture 1: Security goals depicted as Venn diagram

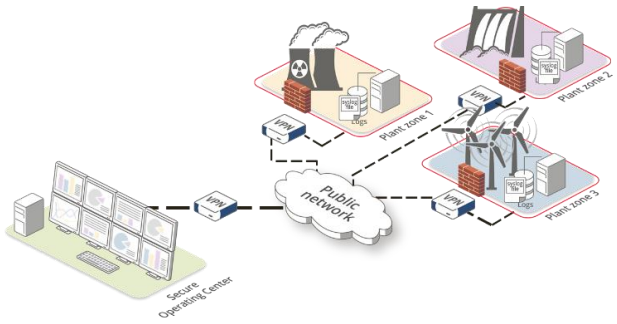
Availability means ensuring timely and reliable access to, and use of information. A loss of availability disrupts the access or use of information or systems. The classic case of an attack on availability is a Distributed Denial of Service attack, such as in the case of Estonia attack.

Confidentiality covers data confidentiality and privacy. It is the preserving of authorized restrictions on information access and disclosure, including means of protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information, as in the case of Manning and Snowden.

Integrity covers both data and system integrity. It entails the guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information, repudiation and authenticity, such as an attack on a Supervisory Control And Data Acquisition (SCADA) system.

Picture 1 depicts the security areas as a Venn diagram. The intersection of the tree sets, gay area in Picture 1, is the security goal of any security. Ideally, the security goal is extended to also incorporate data origin authentication.

Data origin authentication can be achieved using a secure Virtual Private Network (VPN). By implementing secure VPNs, control systems can e.g. send status and log information without leaking sensitive information, see example in Picture 2. This prevents attacks or manipulation of infrastructure, and enables the safe monitoring of surveillance cameras from a central site.



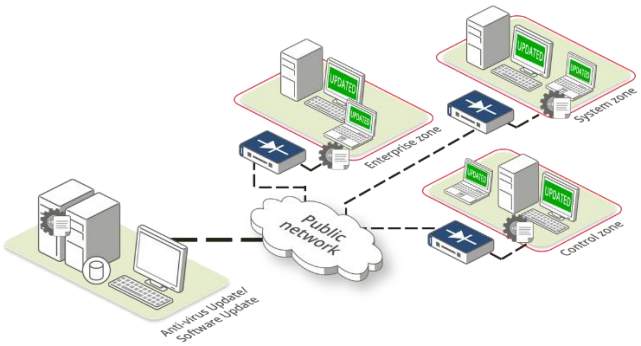
Picture 2: VPN in SCADA system

VIII. PREVENTING HUMAN INTERFERENCE

In high security environments, set regulations often require that networks hosting classified information are isolated from other networks, effectively creating zones of different security clearances. However, there are times when these networks need to be made accessible, for instance when information needs to be transferred to them. The ability to transfer information to a classified network is vital for organizations such as military and government agencies. It is equally vital in industrial control system (ICS) environments managing critical infrastructure, such as utilities or public transportation operators.

Moving information manually, by exporting information onto a USB stick or a CD and importing it into the secure network, is a tedious process that does not provide real-time transfer, and opens up to human error or sabotage. It is thought that Stuxnet was introduced using a USB stick. Stuxnet propagation routines never make an attempt to spread to random targets for example by generating random IP addresses. Everything happens within the confined boundaries of a trusted network. However, trusted environments, even air gapped, aren't necessarily secure anymore. Contractors working at the Iranian nuclear power plant work for other clients as well, and they will have carried their Stuxnet infected laptop computers to those clients and connected them to their secure networks, however ill advised that may be from a security perspective.

A data diode, a smart, one-way information transfer device, connects two networks of different security levels eliminating any possibility of information being sent in the opposite direction of the transfer, shielding the network and its information from external manipulations and attacks. Picture 3 depicts a logical network design where data diodes are used to for distribution of antivirus/software updates while ensuring that confidential information within a the protected zone are truly kept within the protected zone.

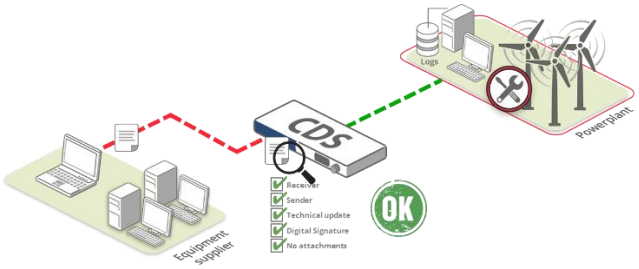


Picture 3: Data diode for secure antivirus/software updates

Bidirectional information exchange between two networks of different security levels can only be realized if information flow control is guaranteed.

This can be guaranteed by implementing in a Cross Domain Solution (CDS) with high assurance design. It enables bidirectional-filtered transportation of data between different security domains by acting as a boundary protection device.

A simple example is highlighted in Picture 4. Here the windmill is in need of service e.g. software update. The equipment supplier sends the software update to the windmill. The software update is filtered and send securely via a Cross Domain Solution. Only explicitly approved information is allowed to pass through the CDS. It is quiet trivial to design secure networks where CDS ensures that not even contractors mobile devices connected, intentionally or unintentionally, to the secure network can cause any damage.



Picture 4: Cross Domain Solution

When geographically scattered networks of *similar* security levels need to share information and data over open networks, such as the Internet, they need to assure that their communication is protected from eavesdropping, manipulation and fabrication. By utilizing hardware based network encryptors organizations are able to create encrypted tunnels through open networks, such as the Internet. Encrypted tunnels, Virtual Private Network (VPN), prevent all kinds of unauthorised data access and manipulation. Thus, secure tunnels enable organisations to securely exchange classified information over the Internet. By combining VPN with CDS, geographically scattered networks of *different* security levels are able to exchange information securely without the risk of unauthorized disclosure of classified information.

The term Digital Pearl Harbor predicts a world where hackers could launch several attacks on critical infrastructure at one time that could actually destroy physical infrastructure, as opposed to just simply disrupting or exploiting digital information and communication. Stuxnet appears to demonstrate such an attack. However with the right countermeasures in place, we can hopefully prevent further attacks.

While some would say it was difficult, or even impossible to prevent determined cyber militia, or individuals like Snowden and Manning from compromising a system, new emerging technology is available today to prevent this.

LITERATURE

[1] UK cabinet office, Cyber security policy, https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace

Johan L. Eliasson is Vice President and Regional Manager for Central Europe at Advenica AB (previously Business Security). Previously he had leading positions in the aerospace and security industry, among others as Vice President Industrial Cooperation, Saab AB. Since 2010 until present he has been President of the Swedish-Austrian Chamber of Commerce in Austria. He holds Bachelor in Aerospace Engineering from Princeton University, USA and MBA from INSEAD, France.

Stefan Chevul is a technologically skilled product manager who excels at bridging business, technology and user experience. Passionate about discovering products that are valuable, usable and feasible while maximizing business value. Stefan holds a Tec.Lic. degree in telecommunication systems and also a M.Sc. in Electrical Engineering. He currently works at Advenica AB where he manages the VPN product portfolio.

Martin Nordqvist holds Bachelor in Business Administration from Malardalen university, Sweden. He finished Executive training at INSEAD, France and exchange studies at Universidad Adolfo Ibanez, Chile. Martin has been in IT industry for 15 years with executive sales positions within IBM and as managing partner in a consultancy company. Since January 2014 he has benn sales director – product and services and member of executive management team at Advenica AB.

Kako zgraditi kritično infrastrukturo v dogovorjenih časovnih, vsebinskih in denarnih okvirjih

Tomaž Aljaž, EMA d.o.o., Celje

Povzetek — S sedanjim manjšanjem sredstev za investicije in zaostreno konkurenco poizkuša vsak potencialni ponudnik izgradnje (kritične) infrastrukture ponuditi najnižjo, a komaj vzdržno ceno. Tega se podjetja močno zavedajo, zato iščejo načine, kako se izboljševati čim bolj racionalno, na način, ki bo prinesel želene rezultate. V prispevku se bomo osredotočili na orodja in aplikacije, poznane pod skupnim imenom "teorija omejitev" (ang. Theory of Constraints – TOC). Orodja in aplikacije so osredotočene na vpeljavo samo nekaj, vendar najpomembnejših izboljšav, ki prinašajo največji učinek. Z namenom, da odgovorimo na vprašanje, »kako zgraditi kritično infrastrukturo v dogovorjenih časovnih, vsebinskih in denarnih okvirjih«, si bomo pomagali in iskali ne-fizične omejitve (politika dela, pravila, merila) z orodji t.i. miselnega procesa teorije omejitev. Za iskanje fizičnih omejitev (ljudje, stroji) pa bomo uporabili orodja, ki omogočajo skrajšanje časa, potrebnega za izvedbo projektov, izboljšanje kvalitete izvedbe projektov in posledično izboljšanje finančnih rezultatov podjetij, vpletenih v izgradnjo (kritične) infrastrukture, zadovoljstvo države (zadovoljni zaposleni in povečani prihodki v državni proračun) in zadovoljstvo državljanov (kot uporabnikov storitev, izvedenih s projekti). Prikazali bomo tudi iniciativo reforme javnih del na Japonskem, imenovano »Win-Win-Win«, ki se je začela okoli leta 2000 in dosegla skrajšanje izvedbe projektov za več kot 20 %, povečala sodelovanje med izvajalci in državo in povrnila zaupanje v državne institucije. Na osnovi pozitivnih izkušenj na Japonskem bi lahko razmislili in začeli iniciativo, kjer bi uporabili uporabljene pristope v domačem okolju. Tako bi z vpeljavo navedenih principov izvajanja projektov (kritične infrastrukture) na nivoju države lahko izvajalci (kritične) infrastrukture pridobljene izkušnje na domačem trgu prenesli tudi v izvedbo projektov v tujini. Z uporabo nove metode izvajanje projektov bi pridobili zadostno konkurenčno prednost pred drugimi (tujimi) podjetji, ki uporabljajo tradicionalne pristope. S tem bi pridobila tudi država.

Ključne besede — kritična infrastruktura, teorija omejitev, upravljanje z viri, agilno projektno vodenje, projektno vodenje s kritično verigo, optimiziranje procesov

Abstract — With recent reduction in investments of the Government and increased competition, many companies involved in (critical) infrastructure works are bidding at cost or lower, just to fill their order books. Companies are aware of this fact and they are looking for different ways how to improve on most rational way. In the article we will focus on tools and applications provided by Theory of Constraints (TOC), which brings approach that enables organization to recognize few important from many trivial points that needs to address in order to achieve competitive advantage (e.g., shorten project duration, improve quality of deliverables). In order to find solutions to our question »how to build critical infrastructure in defined scope, time and budget«, we will use tools and applications of Thinking process to find un-physical constraints (e.g., policy, rules, measurement) and several other tools addressing physical constraints (people, machines) to improve throughput of companies deliverables, improve satisfaction of the Government (employees, more income) and residents (users of the services delivered by projects). Additionally, we will show main areas of »Win-Win-Win Public Work Reform« in Japan that started in mid-2000. It showed more than 20% reduction of time needed to deliver project, improve teamwork between companies and Government officials and return trust in government institutions. With introduction of new project methodology in Government projects can encourage companies to use them at home and then use skills they have learned and practiced at home, to win contracts abroad and exploit decisive competitive edge over companies that use traditional methodologies. By winning more contracts government can only benefit – more income. There is win-win solution for all.

Keywords — Critical infrastructure, Theory of Constraints, constraint management, agile project management, Critical Chain Project Management, process optimization

I. UVOD

Z zmanjšanjem vlaganj v izgradnjo (kritične) infrastrukture s strani države zaradi finančne krize, se je število projektov v zadnjih letih zelo zmanjšalo. To je povzročilo, da je veliko podjetij v težavah ali da so celo v stečaju. Po drugi strani pa se je povečalo število priložnosti, kjer bi podjetja lahko delala. V ta namen se srečujemo z veliko iniciativami, ki smo jih zasledili pri sorodnih ali konkurenčnih podjetjih in na državnih nivojih, vendar žal z njimi doma ne dosežemo pričakovanih rezultatov. Razlogov je lahko več, od tega, da so vpeljane izboljšave v konfliktu z obstoječim načinom vodenja, pravili ali pa merili, ki veljajo. Na osnovi tega lahko trdimo, da ni dovolj, da samo vpeljemo novo rešitev v obstoječi sistem, pač pa moramo vedeti tudi kateri del sistema bomo nadgradili oz. zamenjali. Pri tem moramo natančno razmisliti in vedeti katere novosti moramo vpeljati in kateri deli sistema ostanejo nespremenjeni.

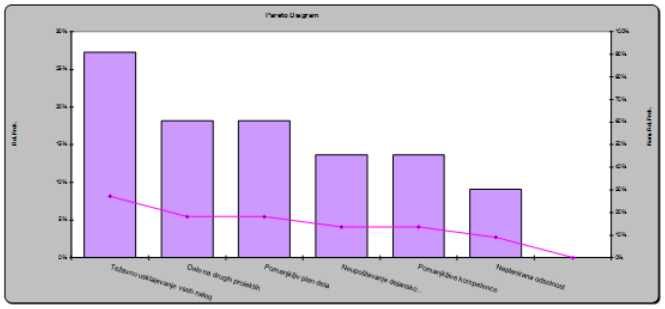
Na osnovi navedenega vidimo, da potrebujemo sistematičen pristop k reševanju problematike. Pogledati je potrebno trenutno stanje in določiti, kaj je potrebno spremeniti ter predlagati smer rešitve. Na koncu pa sledi zelo pomembna odločitev, kako izvesti implementacijo načrtovanega.

II. TEORIJA OMEJITEV

Odgovore na navedena vprašanja bomo iskali s pomočjo metodologije, ki jo je v začetku osemdesetih let prejšnjega stoletja začel vpeljevati dr. Eliyahu M. Goldratt in jo je poimenoval »teorija omejitev« (Theory of Constraints – TOC) [1]. Le-ta predpostavlja, da v vsaki organizaciji obstajajo številni procesi (viri), ki so med seboj povezani in soodvisni. Delovanje organizacije se primerja z močjo »verige«, kjer je moč celotne verige omejena z močjo najšibkejšega člena. V primeru organizacije to pomeni, da so njeni rezultati odvisni od hitrosti izvedbe nalog določenega procesa, vira oz. pravila, ki je »najšibkejši«. Najšibkejši člen predstavlja sistemsko omejitev organizacije in omejuje doseganje boljših rezultatov. Posledično to pomeni, da kakršne koli izboljšave na členu, ki ni najšibkejši, (običajno) ne zagotavljajo izboljšav – lahko pa povzročijo še več

negativnih posledic (npr. kopičenje zalog nedokončanega dela).

Kot je navedeno v [5] običajni pristop vpeljevanja izboljšav temelji na spisku trenutnih težav in problemov, ter razlogih za odstopanje med trenutnim stanjem in našimi pričakovanji oz. plani. Razlogi za odstopanje so običajno zavedeni v Paretovem diagramu, od katerih najpogostejši postanejo predmet izboljšav, ali analizi SWOT kot je prikazano na sliki 1.

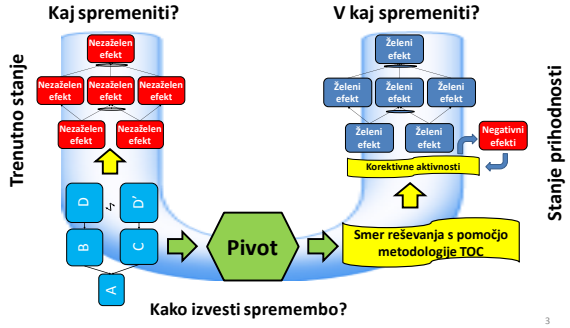


Slika 1: Primer Paretovega diagram najpogostejših razlogov za odstopanje od želenega stanja

Navedeni pristop ne upošteva bistvenega dejstva, da so razlogi za odstopanje med seboj soodvisni. Izvajanje izboljšav, brez upoštevanja soodvisnosti, namreč pripelje le do manjših pozitivnih rezultatov, saj se kmalu po vpeljavi »izboljšave« pokaže, da so navedena odstopanja samo nekakšni simptomi bolj globokega in večjega problema. Reševanje simptomov nam neznanih problemov ne vodi k trajni rešitvi, ampak lahko vodi celo do izvajanja aktivnosti, ki se ne bi smele izvesti. To pomeni, da potrebujemo logičen in strukturiran pristop, ki nam bo omogočil zaznati ključni problem in pokazal načine, kako ga eliminirati, ne da bi povzročil nove probleme.

A. *Miselni proces Teorije omejitev*

Na osnovi teh spoznanj lahko rečemo, da najpomembnejši del Teorije omejitev predstavlja t. i. »miselni proces« (ang. Thinking Process) [2] ki se osredotoča na razreševanje nefizičnih omejitev v organizacijah, kot npr. politika dela, pravila, kultura podjetja, merila. Miselni proces zagotavlja orodja, s pomočjo katerih lahko najdemo ključne probleme in njihove posledice (po načinu vzrok – posledica) ter rešujemo konfliktne situacije, ki jih moramo izvesti v sklopu vpeljevanja izboljšav. S pomočjo njih lahko odgovorimo na vprašanje »kaj spremeniti?«, »v kaj spremeniti?« in »kako izvesti spremembo?« ter »kako doseči nenehne izboljšave?«.



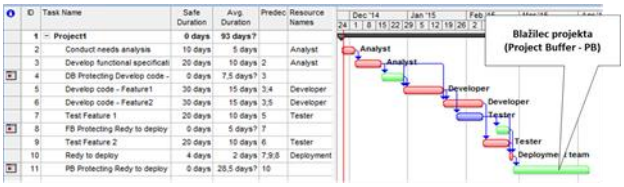
Slika 2: Miselni proces TOC v obliki U

Kot prikazuje slika 2 [4], je miselni proces razdeljen na 3 področja: na levi strani so navedene stvari, ki jih moramo spremeniti; na desni strani v kaj jih želimo spremeniti in na sredini koraki, ki jih moramo izvesti, da lahko pridemo v želeno stanje. Da to lahko storimo moramo uporabiti vse svoje znanje, razumeti vse elemente rešitve in kako so elementi med seboj povezani oz. soodvisni. V nasprotnem primeru je implementacija izboljšav skoraj nemogoča.

Začeti moramo analizo obstoječega stanja in nezaželenimi efekti, s katerimi se organizacija (ali njen del) srečuje. Na osnovi tega dobimo vizualno razumevanje obstoječega delovanja organizacije in ugotovimo, kaj moramo spremeniti. Nato nadaljujemo z reševanjem navedene problematike z ugotovitvami, kaj moramo spremeniti oz. nadomestiti in katere iniciative v obstoječem okolju izvesti, da lahko pridemo do želenih rezultatov. Tako dobimo strateško usmeritev in korake, katerih središče rešitve je zavedeno v t.i. pivotu.

B. *Projektna metodologija kritične verige*

Projektna metodologija kritične verige (ang. Critical Chain Project Management - CCPM) [7] je poznana metodologija za upravljanje projektov kot del orodij in aplikacij metodologije Teorije omejitev. Posebnost CCPM je v tem, da se za planiranje projekta uporabijo agresivni časi izvedbe z upoštevanjem 50 % zanesljivost ocene potrebnega časa za izvedbo nalog, negotovosti posameznih nalog pa združi na nivoju projekta v t.i. blažilcu projekta. Poleg tega odgovarja na problematiko obnašanja posameznikov med izvajanjem projekta kot npr t. i. študentskega sindroma (»kar lahko prestaviš na jutri, prestavi na jutri«) in Parkinsonovega zakona (»če sem rekel, da bo naloga končana v petek, bo naloga končana v petek« – zapolnijo ves razpoložljiv čas).



Slika 3: Primer projektnega plana po metodologiji kritične verige

C. *Večprojektno okolje*

Kot smo omenili na začetku poglavja, je moč verige tako močna kot najšibkejši člen verige. V primeru projektov predstavlja najšibkejši člen t.i. kritična veriga projekta. Kritična veriga projekta predstavlja nadgradnjo definicije kritične poti projekta, saj upošteva poleg najdaljšega zaporedja soodvisnih nalog projekta še vire s katerimi se bodo naloge izvedle.

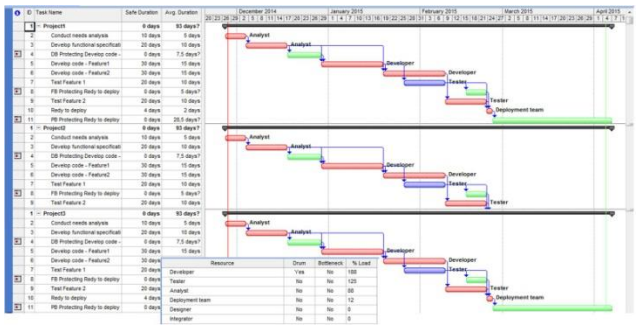
Za izboljšano upravljanje projektov in projektnega portfelja z deljenimi viri uporabljajo t.i. »pet korakov fokusiranja«, ki jih predpisuje teorija omejitev. Le-ti omogočajo izboljšati rezultate dela organizacije in iztržiti največ, kar je možno glede na trenutno kapaciteto virov z minimalnimi investicijami. Koraki so sledeči [5]:

- Korak 1: Identificiraj ključno omejitev (kritična veriga);
- Korak 2: Določi plan dela za ključni omejitvi (pospešiti naloge na kritični verigi);
- Korak 3: Podredi delo preostalih, da bodo ključni viri na kritični verigi vedno imeli delo;
- Korak 4: Izboljšaj (okrepi) kritično verigo (Razbremenite vire na kritični verigi z »nepotrebnimi« nalogami);
- Korak 5: Pozor! Če se ključna omejitev spremeni,

začni pri koraku 1 (spremenite pravila, postanite boljši in boljši).

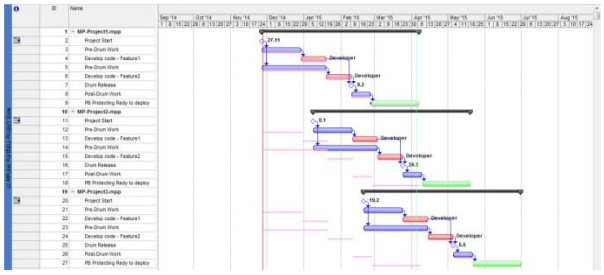
Identifikacija ključnega vira v projektni organizaciji, ki je fizične narave, je razmeroma enostavna in se lahko zelo pragmatično določi. Običajno nam pri določitvi ključnega vira pomaga programska oprema za planiranje in spremljanje izvedbe (nalog) projektov, iz katere lahko pridobimo navedene informacije ali pa je odločitev o ključnemu viru sprejeta na nivoju vodij organizacijskih enot.

Kot primer si oglejmo sliko 4, ki ponazarja tri med seboj soodvisne projekte (Project1, Project2 in Project3) in si delijo skupne vire. Pri tem smo izvedli plan projekta po projektni metodologiji CCPM.



Slika 4: Portfolio projektov s soodvisnimi viri izveden s programski orodjem cc-(M)Pulse [8]

Na navedenem primeru lahko razberemo, da je ključni vir »Developer«, ki je v danem obdobju 188% obremenjen. S tem, ko smo identificirali ključni vir, moramo določiti, kako ga bomo uporabili znotraj našega projektnega portfelja. V ta namen je potrebno pripraviti, glede na cilje organizacije, podroben plan njegovega dela.

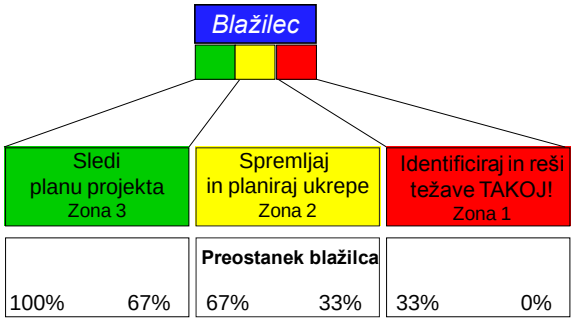


Slika 5: Princip izvedbe plana projektov v večprojektnem okolju z upoštevanje ključnega vira

Vsekakor je nesmiselno, da planiramo ključni vir na več projektih istočasno in že v samem planu povzročamo konflikt med projekti. Dosti bolje je, da izvedemo plan projektov glede na razpoložljivost kritičnega (strateškega) vira, pri tem pa prioritiziramo projekte med seboj – planiramo in razporedimo projekte eden za drugim glede na razpoložljivost ključnega (strateškega) vira. Pri tem pa se moramo izogibati (negativni) večopravilnosti oz. dodeljevanju prevelike količine nalog, ki jih ključni vir ne more izvesti (slika 5). Vemo, da ključni vir diktira rezultate nalog projekta oz. celotnega portfelja projektov, zato vsak dan izgubljen na njem pomeni dan izgubljen na nivoju projektov (v katere je vpleten). Torej mu je potrebno zagotoviti konstantno in zadostno količino dela. Posledično to povzroči, da se morajo vsi preostali vpleteni v projekt podrediti njegovemu delu (zagotoviti, da v določenem trenutku morajo biti na voljo vse stvari, ki jih ključni vir potrebuje za izvedbo svojih nalog projekta).

Kot rezultat navedenega vidimo, da določeni viri, ki so pred ključnim virom (Pre-Drum Work) ne smejo delati nalog, ki bi povzročile povečanje količine aktivnih nalog namenjenih ključnem viru (naloge se izvajajo v načinu »As-Late-As-Possible (ALAP)«. S tem pa naletimo na prvo težavo meril (pravila, politika) dela v podjetjih, kjer je »učinkovitost« virov merjena glede na 8-urni delavnik (40 ur na teden). V takšnih okoljih vodje in vodstvo pričakuje od svojih podrejenih, da so vedno »zaposleni« – če nimajo dela, se jim ga pa najde! Reševanje omenjene situacije zahteva spremembo v delovanju in organizacijski kulturi organizacije, kar pa ni najlažje vpeljati. Potrebna je sprememba razmišljanja v smer, da so prva prioriteta rezultati podjetja in ne »učinkovitost« posameznih virov ali oddelkov. Posledično se mora podjetje sprijazniti z dejstvom, da ne-ključni viri ne bodo polno zaposleni in bodo imeli nekaj »prostega časa«. Znotraj tega časa se lahko izobražujejo, pomagajo pri nalogah dodeljenih ključnim virom, prevzamejo določeno delo, izvajajo aktivnosti povezane z izboljšavami procesov/dela, preventivno vzdrževanje, ipd.

Izboljšanje izvedbe projektov in portfelja projektov nam dodatno omogočajo še upravljanje »blažilcev« oz. njihovo zajedanje. Blažilec je razdeljen na tri področja: zeleno, rumeno in rdeče, kot je prikazano na sliki 6. Zelena barva pomeni, da je projekt znotraj predvidenih časovnih rokov, medtem ko rumena barva pomeni, da je potrebno pogledati zakaj je prišlo v zajedanje v rumeno zono in začeti pripravljati korektivne ukrepe. Rdeča barva blažilca projekta pa pomeni, da so resne težave na vidiku in je potrebno takojšnje ukrepanje, saj bo nadaljnje ignoriranje statusa blažilca pomenilo zamudo na projektu.



Slika 6: Blažilec razdeljen na tri področja

Spremljanje statusa blažilcev projekta(ov), običajno predstavljenim v t.i. Fever chart [3] (slika 13), nam omogoča hitro reakcijo v primeru pomanjkanja dela na ključnem viru, ki lahko nastane zaradi sprememb v zadnjem trenutku ali nepredvidenih težav (Murphy). Ker imajo vsi ne-ključni viri večje zmožnosti od ključnega vira, se lahko hitro odzovejo na stanje blažilca. V primeru, da pride do zajedanja blažilca v kritično (rdečo) zono enega projekta, potem se morajo hitro izvesti korektivne akcije – pozitivna večopravilnost (»premestitev« virov iz enega projekta na drugega). Na ta način se (lahko) projekt vrne v dogovorjene okvirje.

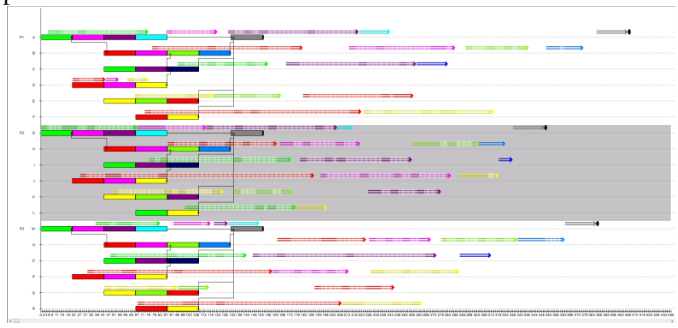
III. ZAKAJ TRADICIONALNO VODENI PROJEKTI MNOGOKRAT NE DOSEŽEJO ŽELENIH REZULTATOV?

Zelo težko je primerjati izvedbo istega projekta po klasični metodologiji in metodologiji kritične verige ter spreminjati parametre, saj ne moremo zagotoviti istih

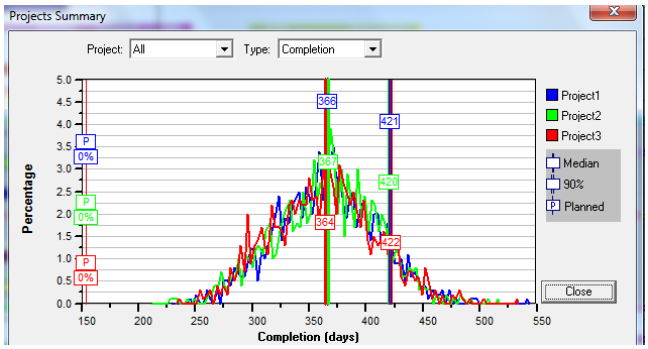
pogojev (tudi če imajo isto vsebino), preveč je izgovorov in razlogov za odstopanje, preveč je spremenljivosti v nalogah projekta in se vsaka rešitev (problem) spreminja sproti. Dosti bolje je, če lahko s pomočjo simulatorja analiziramo projekt ali skupino projektov večkrat in pogledamo trende ter spreminjamo različne parametre. V ta namen si bomo pomagali s PmSim simulatorjem [6].

Na spodnjih slikah so prikazani rezultati simulacije izvedbe projektov v večprojektnem okolju na dva načina – na klasičen način in s pomočjo metodologije kritične verige.

Vsak projekt ima predviden čas izvedbe 152 dni (konec označen s črnim krogom za sivim kvadratom), viri (barva določa vir) so med projekti deljeni, vključen je študentski sindrom in 75 % virov napačno poroča predčasno dokončanje naloge (Parkinsonov zakon). Simulacija je izvedena s 1000 ponovitvami.



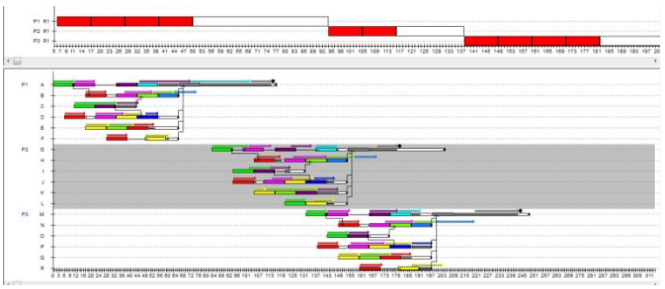
Slika 7: Rezultati simulacije izvedbe projektov po klasični metodologiji



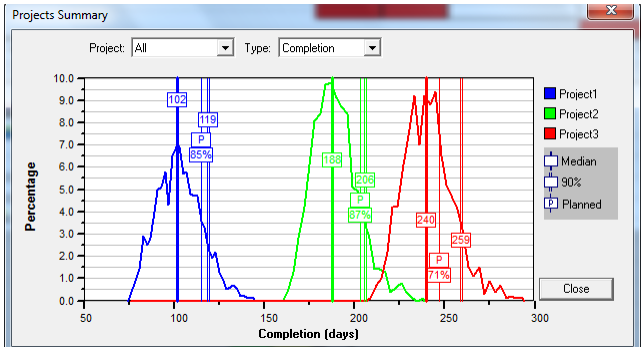
Slika 8: Čas dokončanja projektov po klasični metodologiji

Ne glede na to, da gre za prikaz simulacije, vidimo, da nobeden izmed projektov po klasični metodologiji ne bo dokončan v predvidenem roku (slika 7 in slika 8). Predviden čas dokončanja projekta je daljši za več kot trikrat glede na planiran čas izvedbe (iz predvidenih 152 dni na 422 dni z 90 % zanesljivostjo).

Na sliki 9 smo izvedli plan projekta po metodologiji kritične verige in določili ključen vir (rdeča barva) na nivoju portfelija projektov. Le-ta je povzročil, da so se plani projektov po prioriteti podredili njegovi razpoložljivosti. Prav tako smo dodali še dodaten blažilec (100%) med posameznimi projekti za zaščito ključnega vira (tudi ključni vir ima spremenljivost izvedbe nalog projekta) – blažilec ključnega vira (ang. Drum Buffer – DB).



Slika 9: Rezultati simulacije izvedbe projektov v večprojektnem okolju po metodologiji kritične verige



Slika 10: Čas dokončanja izvedbe projektov po metodologiji kritične verige

Kot je razvidno is slike 10, so časi dokončanja vseh treh projektov bistveno krajši. Prvi projekt je z 90 % zanesljivostjo končan v 116 dneh, drugi v 176 dneh, tretji pa v 212 dneh. Vsi trije projekti so izvedeni skoraj dvakrat hitreje kot v primeru, ko viri izvajajo večopravilnost med projekti – z 90% zanesljivostjo je prvi projekt izveden v 116 dneh oz. ~28% časa (116/421), drugi v 206 dneh oz ~49% časa (206/420) in tretji v 259 dneh oz. ~61% časa (259/422). Prednosti na nivoju podjetja so očitne, saj se projekti lahko začnejo bistveno hitreje tržiti in izboljšamo denarni tok podjetja.

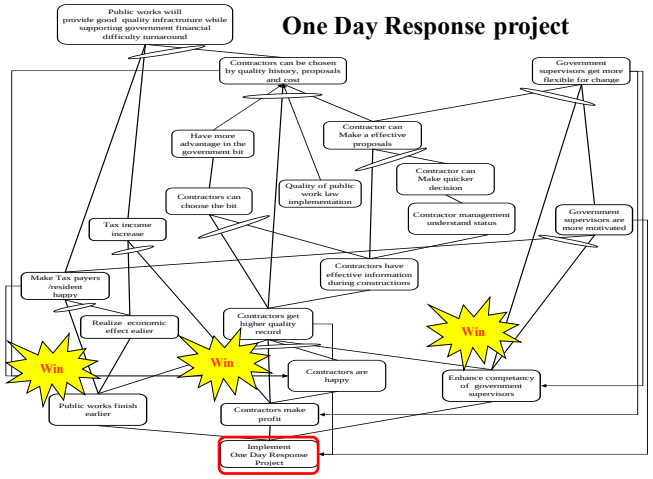
IV. PROJEKT JAVNIH DEL NA JAPONSKEM »WIN-WIN-WIN«

Poznavanje pristopa izvajanja izboljšav izvedbe javnih del na Japonskem nam lahko pomaga pri definiranju strategije izgradnje (kritične) infrastrukture (*Standing on the Shoulders of the giants* [9]) v Sloveniji. Na Japonskem so se v začetku tisočletja lotili sprememb izvajanja javnih del / projektov pod okriljem Hokkaido regional Bureau of Ministry of Land, infrastructure and transportation (MLIT) [9]. Pri razreševanju omenjene problematike so si pomagali z orodji t.i. miselnega procesa Teorije omejitev, s pomočjo katerih so lahko odgovorili na vprašanje »kaj spremeniti?«, »v kaj spremeniti?« in »kako izvesti spremembo?

Najprej so se lotili analize trenutnega stanja in nezaželenimi efekti, s katerimi se srečujejo. Zaznani so bili trije glavni nezaželeni efekti: država ima finančne težave (premalo prihodkov glede na odhodke), majhni profiti izvajalcev javnih del (velikokrat delajo z izgubo oz. komaj pokrijejo stroške) in slaba usposobljenost za delo zaposlenih v javni upravi. Prav tako so izvajalci javnih del izpostavili velike težave vezane na dolgotrajne (in časovno potratne) postopke kadar so bile potrebne povratne informacije s strani vladnih inštitucij zaradi sprememb (npr. zaradi naravnih okoliščin) ali nepričakovanih težav med samo izvedbo del projekta. (Pre)pozne povratne informacije so povzročile

(velike) časovne zamude pri izvedbi projektov in posledično prekoračitve planiranih stroškov, kar je dodatno negativno vplivalo na vse vpletene (izvajalce in njihove podizvajalce, državo in državljane).

Na osnovi analize nezaželenih efektov in razlogov za njihov obstoj s pomočjo orodij miselnega procesa Teorije omejitev so definirali, kaj morajo spremeniti. Potrebni so bili hitri odgovori od vladnih inštitucij, na osnovi katerih so lahko izvajalci sprejemali odločitve in omogočili, da ne bo prihajalo do zamud na projektih. Preverjanje predlaganih sprememb so izvedli s pomočjo orodja t.i. drevesa želenega stanja (ang. Future Reality Tree), kot prikazuje slika 11 – definirali so iniciativo, ki so jo imenovali »odgovor v enem dnevu« (ang. One Day Response Time).



Slika 11: Preverjanje iniciative »odgovor v enem dnevu« s pomočjo miselnega procesa Teorije omejite in uporaba orodja »drevo želenega stanja« [11]

Cilj iniciative je omogočiti hitrejši odziv vladnih inštitucij do podjetij, ki izvajajo javna dela in vpeljavo projektne metodologije, ki bi omogočila skrajšanje časa potrebnega za izvedbo projektov. Tako so dobili nekaj najpomembnejših strateških usmeritev, ki lahko ob uspešni implementaciji prinesejo največji doprinos v najkrajšem času.

A. *Iniciativa »Odgovor v enem dnevu«*

»Odgovor v enem dnevu« je simbolično ime, ki izvajalcu projekta določa na strani države odgovornega vladnega uslužbenca. Le-ta nudi pomoč izvajalcu in poizkuša čim bolj zmanjšati zakasnitve vezane na pričakovane povratne informacije s strani naročnika (države) oz. različnih državnih institucij. Vendar to ne pomeni, da bo le-ta podal celotno rešitev na izpostavljeno problematiko v enem dnevu. Ampak, da se poizkuša rešiti čim več odprtih stvari v enem dnevu in komunicirati z izvajalcem koliko časa lahko čaka na polno informacijo. Pri tem pa je ključnega pomena, da se med vpletenimi vzdržuje komunikacija in da se držijo dogovorjeni roki med vpletenimi ter se ne vnašajo dodatne zamude na projektu. To omogoča izvajalcu ustrezno planiranje nadaljnjih aktivnosti na projektu in zmanjšanje rizikov na projektu ter zamud.

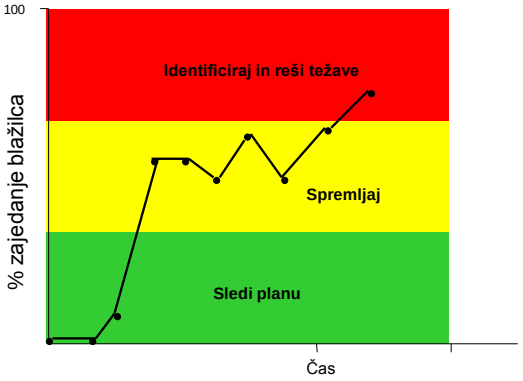
B. *Projektna metodologija kritične verige*

Omenjena iniciativa »odgovor v enem dnevu« ni predpisovala točno določene metodologije projektnega vodenja. Kljub vsemu pa so po končanem prvem projektu (reka Tonebetsu leta 2004) naredili evalvacijo uspešno (predčasno) dokončanega projekta in prišli do spoznanja, da je uporabljal zelo podobno metodologijo, kot jo sedaj poznamo pod imenom projektna metodologija kritične verige. To je bil tudi vzrok, da je večina izvajalcev začela slediti tej metodologiji in jo začela uporabljati pri izvedbi projektov zaradi skrajšanja časov izvedbe ter z javnostjo deliti cilje, rezultate in kriterije za uspešno dokončanje projekta (slika 12).

Slika 12: Javno predstavljeni cilji, rezultate in kriterije za uspešno dokončanje projekta [11]

C. *Medsebojno sodelovanje na nivoju projekta*

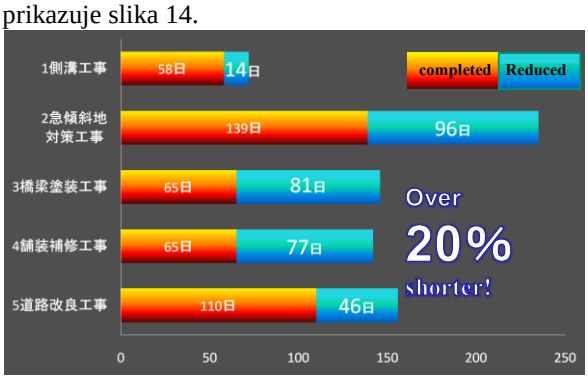
Projektni plani, ki uporabljajo projektno metodologijo kritične verige, imajo na koncu projekta blažilec projekta (slika 3). Kot smo omenili v prejšnjem poglavju, spremljanje zajedanja blažilca in posledično njegove barve v kombinaciji z opravljenim delom (na kritični verigi projekta) omogoča izboljšanje upravljanje projekta. Spremljanje zajedanja blažilca nam omogoča že v zgodnjih fazah projekta zaznati težave in spremljati katere naloge povzročajo njegovo zajedanje (slika 13). S tem, ko vemo katera naloge povzroča (potencialne) zamude, lahko začnemo hitro izvajati korekcijske aktivnosti, preden je prepozno.



Slika 13: Spremljanje zajedanja blažilca glede na kritično verigo projekta – ang. Fever Chart

Upravljanje blažilcev so znotraj iniciative »odgovor v enem dnevu« uporabili kot način komunicira stanja projekta in jasno pokazali soodvisnosti izvedbe nalog / zadolžitev med vpletenimi – podjetje, ki je zadolženo za izvedbo (kritične) infrastrukture, deli zajedanje blažilca z odgovornim vladnim uslužbencem za omenjeni projekt. Če je povratna informacija s strani državnih inštitucij pomembna za nadaljevanje projekta, se vse zakasnitve zaradi manjkajoče povratne informacije takoj rezultirajo v zajedanju blažilca (običajno na slabše). Zavedanje o pomembnosti povratnih informacij pri odgovornemu vladnemu uslužbencu (in vladnih inštitucijah) se je povečalo, kakor tudi zagotavljanje

ustreznih podatkov in sprejemanje odločitev. Upravljanje zajedanja blažilca(ev) projekta je izboljšalo komunikacijo in timsko delo med vpletenimi ter izboljšalo rezultate projektov, kot prikazuje slika 14.



Slika 14: Rezultati prvih nekaj projektov – čas izvedbe skrajšan več kot 20% [11]

V. ZAKLJUČEK

S sedanjim zmanjševanjem sredstev za investicije in zaostreno konkurenco poizkuša vsak potencialni ponudnik izgradnje (kritične) infrastrukture ponuditi najnižjo, a komaj vzdržno ceno. Tega se podjetja močno zavedajo, zato iščejo načine, kako se izboljševati čim bolj racionalno, na način, ki bo prinesel želene rezultate. V mnogih primerih odobravanje vedno novih projektov, zgolj dodajanje novih virov in investicij na strani izvajalcev ne prinese želenih rezultatov. Zastavlja se vprašanje, kako lahko izboljšamo upravljanje projektnega portfelja, kako lahko izboljšamo sodelovanje med izvajalci in državnimi institucijami, kako lahko skrajšamo čas za izvedbo projektov, povečamo kvaliteto dela in povečamo dobiček izvajalcev, povečamo prihodke državi in povečamo zadovoljstvo državljanov?

Odgovore na navedena vprašanja smo iskali sistematično s pomočjo aplikacij in orodij poznanih pod skupnim imenom Teorija omejitev (ang. Theory Of Constraints). Teorija omejitev predpostavlja, da je znotraj vsake organizacije mnogo procesov (virov), ki so med seboj povezani in soodvisni. Na ta način se postavlja analogija delovanja organizacije z močjo »verige«, kjer je moč celotne verige omejena z močjo najšibkejšega člena. Najšibkejši člen pa je lahko fizične narave (osebje ali strok) ali pa ne-fizične narave (pravila, merila, obnašanje posameznikov).

V našem prispevku smo prikazali, kako lahko s Teorijo omejitev, še posebno z miselnim procesom definiramo strateške usmeritve, ki imajo na nivoju vpletenih največji doprinos. Prikazali smo, kako lahko s projektno metodologijo kritične verige skrajšamo čas potreben za izvedbo nalog projekta in posledično izboljšamo rezultate izvajalca in njegovo konkurenčno prednost. Projektna metodologija kritične verige pa ni edini pogoj za uspešno dokončanje projekta, potrebno je dobro in učinkovito sodelovanje z državnimi institucijami. Še posebno pomembne se povratne informacije, ki jih potrebuje izvajalec zaradi nepričakovanih težav med izvedbo projekta ali nepredvidljivih okoliščin. Kot pomoč pri razlikovanju pomembnih od manj pomembnih informacij nam pomaga spremljanje projektnega blažilca, ki je del projektne metodologije kritične verige. Če je povratna informacija s strani državnih inštitucij pomembna za nadaljevanje projekta, se vse zakasnitve zaradi manjkajoče povratne informacije takoj rezultirajo v zajedanju blažilca (običajno na slabše). Takoj lahko vidimo, kako se lahko poveča zavedanje pomembnosti povratnih informacij pri odgovornemu vladnemu uslužbencu (in vladnih inštitucijah), da zagotovijo ustrezne podatke in odločitve hitreje. Identično je potrebno zagotoviti tudi s strani izvajalcev. Upravljanje zajedanja blažilcev lahko smatramo kot način izboljšanja komuniciranja in timsko delo med vpletenimi ter posledično izboljšamo rezultate projektov.

Z vpeljavo navedenih principov izvajanja projektov (kritične infrastrukture) na nivoju države bi lahko izvajalci (kritične) infrastrukture pridobljene izkušnje na domačem trgu prenesli tudi v izvedbo projektov v tujini. Z uporabo nove metode izvajanja projektov, bi lahko pridobili zadostno konkurenčno prednost pred drugimi (tujimi) podjetji, ki uporabljajo tradicionalne pristope. S tem bi pridobila tudi država - dobimo Win-Win-Win situacijo za vse vpletene.

LITERATURA

[1] Eliyahu M. Goldratt, Jeff Cox. The Goal: A Process of Ongoing Improvement, North River Press, 2004
[2] Lisa J. Scheinkopf. Thinking for a Change Putting the TOC Thinking Processes to Use, CRC Press LLC, 1999
[3] Mark Woeppel. Projects in Less Time, TOCICO 2009 Conference presentation
[4] Oded Cohen, Managing System – Part1: Structuring system analysis and solution development through the U-shape, TOCICO Webinar 2014
[5] Tomaž Aljaž, Lidija Grmek Zupanc, Branka Jarc Kovačič, Gabrijela Krajnc, Mateja Demšar. Kako s pomočjo Teorije omejitve delati manj, a narediti več, 2014
[6] Programska oprema PMSim version 2.03
[7] Eliyahu M. Goldratt. Critical Chain, North River Press, 1997
[8] Programska oprema cc-(M)Pulse version 4.0.0.0
[9] Eliyahu M. Goldratt, Standing on the Shoulders of the giants - Production concepts versus production applications: The Hitachi Tool Engineering Example, Goldrat Consulting, 2008
[10] Yuji Kishira, Win-Win-Win Public Works reform, 2007
[11] Yuji Kishira, Win-Win-Win Public Works reform, 2012, Objavljeno na http:// http://www.slideshare.net/commonsenseLT/3-1500-yujikishirawinwinwinpublicworks2012 (zadnji ogled 18. 4. 2015)

Dr. **Tomaž Aljaž** je certificiran strokovnjak na področju Teorije omejitev (angl. Theory Of Constraints – TOC) z znanjem in referencami na tem področju. Ima skoraj 18 let izkušenj v gospodarstvu in bančništvu in več kot 7 let izkušenj kot predavatelj doma in v tujini. V zadnjem obdobju daje poudarek izboljšavi rezultatov dela z vpeljavo »vitkih« metodologij dela v multinacionalnih organizacijah, vodenju oddelkov in ljudi, strokovnih ekip, vzpostavitvi meril dela, pripravi celovitih rešitev in vodenju projektov. Svoje znanje s področja vpeljave »vitkih« metodologij dela je v letih 2013 in 2014 izpopolnjeval na Washington State University v ZDA, ki je specializirana za vpeljevanje »vitkih« metod dela v organizacije, projektna vodenja in druge metode, s ciljem izboljšanja rezultatov v podjetjih. Na omenjeni univerzi je bil jeseni 2014 tudi zunanji predavatelj. V aprilu 2014 je pridobil certifikat na mednarodni organizaciji Theory Of Constraints International Certification Organization (TOCICO).

Zagotavljanje telekomunikacijskih storitev v Elesu v rednem obratovanju in v času izrednih razmer

Marija Mrzel-Ljubič, Venčeslav Perko, Goran Uršič, ELES, Ljubljana

Povzetek — Telekomunikacijske storitve za podporo obratovanju energetskega sistema in za zaščito daljnovodov se načrtujejo in izvajajo glede na zahteve, ki izhajajo iz potreb zagotavljanja prenosa električne energije. Da bi lahko zadostili vsem potrebam, se za izvajanje TK storitev uporablja primerna arhitektura omrežja ter primerna tehnološka oprema. Izredno pomembno je, da se cel sistem načrtuje na vseh ravneh na infrastrukturni, transportni kot tudi na storitveni ravni. Izreden pomen pri načrtovanju in izvajanju storitev ima tudi usposobljenost izvajalcev tako v Elesu, kot tudi tehnoloških partnerjev doma in v tujini. Ob pojavu žledoloma v Sloveniji v februarju 2014, so se posebnosti v načrtovanju in izvajanju TK storitev pokazale kot prednosti. Kljub temu, da je bilo veliko daljnovodov in s tem tudi telekomunikacijske infrastrukture prekinjene, pa prekinitev ni vplivala na delovanje TK storitev, na zagotavljanje komunikacije za obratovanje EE sistema in na zaščito daljnovodov.

Ključne besede — žled, daljnovod, telekomunikacijski sistem, elektroenergetski sistem, optične povezave, zanesljivost, razpoložljivost, IP/MPLS, DCN, NG SDH, DWDM

Abstract — In order to support the functioning of the energy system and to protect the power lines, Telecommunication services are planned and implemented in accordance with the requirements arising from the need of providing electrical power transmission. The appropriate network architecture and suitable technological equipment for the implementation of the TK services are used to meet all the specific requirements.

Professional qualifications of the operators in ELES and in the technology partner companies are of the utmost importance in the planning and delivery of services.

In the case of glaze ice in Slovenia in February 2014, particularities of planning and implementation of telecommunication services have proved to be of major advantage. Although glaze ice demolished many power transmission lines and telecommunication infrastructure, the interruption did not affect data transfer and telecommunication services for the operation of the power system.

Keywords — glaze ice, power liner, telecommunication system, energy system, optical lines, availability**,** reliability, IP/MPLS, DCN, NG SDH, DWDM

I. UVOD

V skladu s slovensko energetsko zakonodajo, družba Eles, d.o.o. izvaja varno in zanesljivo obratovanje energetskega sistema. To zajema upravljanje, razvoj, gradnjo in vzdrževanje 400 kV, 220 kV in del 110 kV prenosnih omrežij, ki omogočajo prenos energije od proizvodnih elektroenergetskih objektov do velikih odjemalcev. Naša naloga je usklajeno delovanje s sosednjimi in vsemi drugimi omrežji, ki so povezana v Evropsko združenje sistemskih operaterjev prenosnega omrežja (ENTSO-E).

Kot del prenosnega omrežja, gradimo hkrati z energetsko infrastrukturo tudi lastno telekomunikacijsko infrastrukturo in omrežja, ki so prvenstveno namenjena izvajanju zanesljivih in varnih storitev za potrebe vodenje prenosnega elektroenergetskega omrežja Slovenije in kakovostno obvladovanje poslovnih procesov v Elesu. Del telekomunikacijskih storitev izvajamo tudi za zunanje uporabnike.

Zahteve po zanesljivosti, razpoložljivosti, varnosti in celovitosti prenosa podatkov v našem omrežju so zelo visoke, saj lahko nedelovanje zvez vpliva na vodenje elektroenergetskega sistema ter zanesljivo oskrbo z električno energijo na nivoju celotne države.

II. NAČRTOVANJE TELEKOMUNIKACIJSKIH SISTEMOV V ELEKTROENERGETSKEM OMREŽJU

Namensko komunikacijska omrežja v elektroenergetskem sistemu se od operaterskih omrežij razlikujejo predvsem po specifičnih zahtevah, ki jih zahtevajo posamezne storitve za potrebe obratovanja elektroenergetskega sistema:

- storitve za vodenje (TCP/IP IEC 60870-5-104) od elektroenergetskih objektov do SCADA sistemov v centrih vodenja morajo biti na samo zanesljive, temveč tudi visoko razpoložljive - 99,99% kar pomeni, maksimalno 1 uro nedelovanja storitev na leto,
- zveze za zaščito zahtevajo poleg zanesljivosti in razpoložljivosti tudi kratke zakasnilne čase med obema končnima točkama daljnovoda,
- čezmejne povezave s tujimi operaterji in naprave zaščite še vedno zahtevajo PDH/SDH vmesnike z namenskimi povezavami,
- poslovne komunikacije med posameznimi poslovnimi lokacijami podjetja potrebujejo velike kapacitete (podatki, video, telefonija),
- omogočen mora biti daljinski nadzor posameznih procesnih naprav,
- izpolnjena mora biti zahteva po veliki varnosti in zaščiti IP omrežij in še bi lahko naštevali.

Če dodamo, da so razdelilne transformatorske postaje in proizvodnji elektroenergetski objekti v katerih zaključujejo daljnovodi oddaljeni od naseljenih področij, kjer ni razpoložljive komunikacijske infrastrukture drugih operaterjev, je to razlog zakaj tako domača kot tuja energetska distribucijska podjetja gradijo svoja komunikacijska omrežja.

Visoke zahteve pri zagotavljanju telekomunikacijskih storitev je možno doseči le s pravilnim načrtovanjem in izgradnjo, pri tem je smiselno upoštevati naslednje:

- do posameznega objekta je potrebno zgraditi vsaj dve fizični povezavi,
- prenosni telekomunikacijski sistemi na fizičnih povezavah morajo biti podvojeni,
- zveze morajo biti izvedene v zaščiti,
- naprave prenosnih sistemov morajo biti napajane iz brezprekinitvenih virov,
- telekomunikacijska oprema mora biti nameščena v ustreznih klimatiziranih prostorih, z varovanim dostopom,
- v IP omrežjih je potrebno izvesti dodatno zaščito pred neželenim vdorom,
- vse posamezne dele telekomunikacijskega omrežja je potrebno redno vzdrževati in daljinsko nadzorovati.

V Elesu je zgrajenih 1600 kilometrov fizičnih optičnih povezav, ki so večinoma izvedene v tehnologiji OPGW (Optical Power Ground Wire) kar pomeni, da so optična vlakna umeščena v strelovodni vrvi daljnovoda. Povezave so vzpostavljene z vsemi elektroenergetskimi objekti prenosnega značaja v Sloveniji in v tujini, kot tudi z večino imetnikov optične hrbtenične infrastrukture v Sloveniji (SŽ, Telekom, Dars). Dostopnost do posameznega energetskega objekta po dveh poteh je zagotovljena z uporabo lastne infrastrukture ter z uporabo optičnih povezav ostalih energetskih podjetij in drugih imetnikov optične infrastrukture.

Za nekatere povezave, kjer ni mogoče zagotoviti obhodnih optičnih povezav, so nameščene brezžične širokopasovne povezave. Le-te ne omogočajo velikih prenosnih kapacitet in v primeru prekinitev na optičnih povezavah, ne omogočajo preusmeritev vseh storitev.

Na optičnih povezavah je nameščenih več prenosnih telekomunikacijskih sistemov v obročni ali mrežni topologiji, ki so namenjeni različnim uporabnikom, glede na njihove specifične zahteve. Tako IP/MPLS paketno omrežje zagotavlja vse tipe Ethernet storitev ter IP VPN storitve, predvsem za notranje uporabnike, ki potrebujejo zveze večjih kapacitet in fleksibilnost. Notranje uporabnike delimo na tehnične uporabnike in poslovne uporabnike. Tehnični uporabniki potrebujejo komunikacijske storitve za video nadzor, konferenčne sisteme, prenos podatkov za spremljanje energetskih naprav ter izmenjavo podatkov z drugimi energetskimi podjetji. Komunikacijske storitve za poslovne uporabnike v podjetju zahtevajo stalno prilagajanje omrežnih funkcionalnosti in dinamično spreminjanje kapacitet. Storitve za poslovne uporabnine so: povezovanje podatkovnih centrov, intranet, internet, poslovni LAN, IP telefonija, kontrole pristopov, izmenjava podatkov s poslovnimi partnerji. Viške kapacitet koristijo zunanji uporabniki preko podjetja Stelkom, d.o.o..

Za potrebe vodenja energetskega sistema sta zgrajeni, zaradi posebnih zahtev glede varnosti in zanesljivosti delovanja komunikacijskih storitev, dve namenski med seboj sistemsko neodvisni omrežji, DCN in NG SDH. DCN je namensko IP MPLS omrežje za prenos procesnih podatkov od lokalnih omrežji v energetskih objektih do republiških centrov vodenja, kjer se nahajajo centralni SCADA sistemi. NG SDH omrežje omogoča prenos storitev, tako za PDH in SDH storitve kot tudi Ethernet in MPLS TP storitve. Istočasno služi kot redundantno omrežje za komunikacijske storitve za potrebne vodenje elektroenergetskega sistema. To omrežje je nadomestilo dotrajana TDM-omrežja (FMX in SDH).

Vse naprave, tako tiste v prenosnih sistemih kot tudi napajalne, so modularne izgradnje s podvojenimi vitalnimi funkcijami in daljinsko nadzorljive. Zveze so izvedene v zaščiti in pri izpadu primarne poti omogočajo samodejno preusmeritev na drugo razpoložljivo povezavo.

V IP-omrežjih uporabljamo dodatne varovalne mehanizme za zaščito podatkov (požarne pregrade, NAT, itd.).

DWDM je trenutno le delno implementiran v omrežju ELES-a in predstavlja optično prenosno omrežje tam, kjer ni dovolj razpoložljivih optičnih povezav oziroma za večanje prenosnih kapacitet ostalih TK omrežij.

Zelo pomembno je, da načrtovanje, izvajanje storitev, obratovanje, vzdrževanje ter odpravljanje napak izvajamo z lastnim, izšolanim kadrom, ki pozna specifiko obratovanja in potreb elektroenergetskega sistema. Podvojen nadzorni center za vsa prenosna telekomunikacijska omrežja omogoča spremljanje delovanje vseh zvez ter tudi stanja napajalnih sistemov za potrebe napajanja naših TK naprav. S pripravljenostjo na domu 24/7 lahko dosegamo kratke čase za odpravo napak. Določeno kritično nadomestno opremo imamo na vroči rezervi in takoj dosegljivo, sklenjene pa imamo tudi ustrezne vzdrževalne pogodbe.

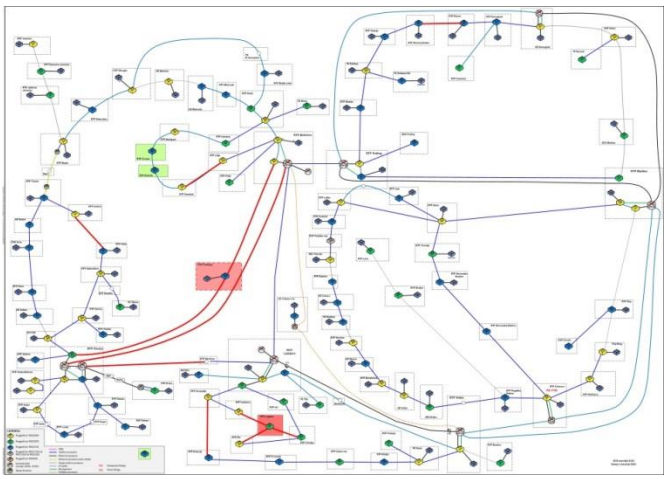
Z vsemi temi ukrepi, vpeljanimi že v procesu načrtovanja in v fazi izgradnje, razpolaga Eles z zanesljivim, dokaj robustnim in fleksibilnim telekomunikacijskim omrežjem, kar se je pokazalo kot prednost pri žledolomu v februarju 2014.

III. DELOVANJE V IZREDNIH RAZMERAH

Izredne razmere kot so npr. žledolom, poplave, potresi,.. lahko močno vplivajo na delovanje celotnega elektroenergetskega sistema, saj lahko povzročijo prekinitev dobave električne energije na širšem področju.

Poškodbe na energetskem sistemu lahko vodijo tudi do prekinitev optičnih povezav ali poškodbe telekomunikacijske infrastrukture. Če bi bile s tem prekinjene tudi zveze od elektroenergetskih objektov do centrov vodenja, bi to pomenilo, da centri vodenja ne razpolagajo več s pravočasnimi in zanesljivimi podatki za obvladovanje elektroenergetskega sistema in ne morejo ustrezno reagirati v izrednih razmerah.

V soboto 1. 2. 2014, se je zaradi žledoloma v popoldanskem času pretrgala OPGW vrv na daljnovodu 400kV Beričevo-Divača. V večernem času se je zaradi povečane obremenitve z žledom porušil preostali del daljnovoda. V Elesu je tako v naslednjem tednu zaradi žleda in poškodb prenehalo obratovati pet visoko napetostnih prenosnih daljnovodov. Porušilo se je veliko daljnovodov in optičnih povezav distribucijskih podjetij, preko katerih ima Eles del fizičnih povezav za svoj telekomunikacijski sistem (glej sliko 1).



Slika 1: DCN omrežje v času žledoloma 2014-prekinitev povezav

Kljub pretrgom fizičnih optičnih povezav na geografsko razpršenih daljnovodih, so zveze za vodenje in obratovanje elektroenergetskega sistema, ki jih zagotavlja Eles preko svojega telekomunikacijskega omrežja delovale nemoteno.

To so omogočile fizične povezave po dveh oziroma več poteh, podvojeni prenosni sistemi, ščitenje zvez na sistemih, ustrezno napajanje (na katerega ne vplivajo nihanja v omrežju), zmogljivi nadzorni sistemi ter predvsem takojšnja odzivnost usposobljenega kadra, vajenega ravnanja v tovrstnih primerih, ki je z ustreznimi manipulacijami preusmerilo promet na razpoložljive povezave vsakič, ko je prišlo do nove, dodatne prekinitve .

Popolnoma so bile prekinjene le zveze iz objektov, kjer so bile pretrgane vse fizične optične povezave zaradi porušene daljnovodne infrastrukture v celoti (npr. Logatec).

Prekinjene so bile tudi storitve za tiste zunanje uporabnike, ki so uporabljali zgolj optično vlakno ali nezaščitene zveze večjih kapacitet, kjer zaradi prevelikih razdalj ali nezadostnih kapacitet ni bilo možno zagotoviti obhodnih poti v okviru obstoječega telekomunikacijskega sistema in optičnih povezav.

Sanacija odprav poškodb žledoloma na daljnovodnem in tudi optičnem omrežju je trajala vse do junija 2014. Pretrgane optične povezave smo ponekod premostili z začasnimi povezavami.

Da smo lahko zagotovili ustrezno razpoložljivost vseh obratovalnih zvez v času odprave posledic havarije, smo za izvedbo obhodne poti začasno najeli optična vlakna pri drugih imetnikih optične infrastrukture.

IV. MOŽNI UKREPI ZA ZMANJŠANJE TVEGANJ NEDELOVANJA STORITEV V IZREDNIH RAZMERAH

Da bi zmanjšali tveganja in škodljive učinke izpadov telekomunikacijskih storitev v primeru izrednih razmer je potrebno v prihodnosti večjo pozornost nameniti tudi nekaterim drugim dejavnikom in ne zgolj izgradnji zanesljivega telekomunikacijskega omrežja:

- Prepoznati je potrebno tiste segmente v omrežju, ki predstavljajo tveganje in lahko bistveno vplivajo na delovanje sistema ter jih spremeniti, dograditi ali zamenjati: npr. neustrezno napajanje, nezadostna kapaciteta na posameznih relacijah, ki ne omogoča preusmeritve, preveliko število naprav v obroču brez prečnih povezav, ena fizična povezava…. Pri tem je potrebno pazljivo načrtovati tudi izgradnjo novih storitev.
- Popolno zaščito fizičnih poti v izrednih razmerah in večjih razsežnosti elektroenergetska podjetja ne morejo v celoti zagotoviti preko svoje infrastrukture. Večina daljnovodov je prosto-zračnih, kjer je možno odpraviti napako od nekaj dni do nekaj tednov, oz. mesecev. V ta namen bi se morali imetniki optične infrastrukture (SŽ, DARS, Telekom, Elektroenergetska podjetja,..) povezati z namenom takojšnjega najema fizične infrastrukture v izrednih razmerah ali izmenjave optičnih vlaken že pri sami izgradnji sistema in ne le pri havariji. Povezave med imetniki telekomunikacijskih omrežij bi morale biti tudi na logičnem nivoju (medomrežno povezovanje) z namenom zagotavljanja obhodnih zvez preko prenosnih sistemov, kjer ni možne izvedbe preko fizičnih povezav. Predpogoj bi bila tudi izgradnja WDM sistema, na katerega bi povezali storitve, ki zahtevajo večje kapacitete. V primeru preusmeritev se namreč potreba po zagotovitvi neodvisne fizične infrastrukture zmanjša.
- Kader je potrebno redno usposabljati, tudi s simulacijami kriznih razmer večjega obsega.
- Potrebno je pripraviti obratovalna navodila za izredne razmere tudi za operaterje na telekomunikacijskih prenosnih sistemih, ki bi bili navezava na obratovalna navodila za energetski sistem.
- Potrebno je preučiti ali bi bilo smiselno vpeljati daljinski nadzor optike na daljnovodih in ga povezati v nadzor elektroenergetskega omrežja z namenom pridobitve pravočasne informacij. Strelovodna vrv z optiko se je zaradi žleda pretrgala nekaj ur pred vodniki, ki so bili zaradi prenosa energije bolj ogrevani.
- V primeru izrednih razmer, ki vplivajo na več segmentov družbe in ne zgolj na elektroenergetski sistem, bi bilo potrebno na nivoju države predpisati nujne ukrepe za ravnanje ob havarijah, kako zmanjšati posledice le-teh, pa tudi kakšen naj bo pretok informacij med posameznimi imetniki infrastrukture, ki je nacionalnega pomena (elektroenergetska infrastruktura, cestna infrastruktura, komunikacije…).

V. ZAKLJUČEK

S pravilnim načrtovanjem omrežja in predvsem z izvajanjem pravih procesov ne moreš preprečiti, da v izrednih razmerah ne bi prišlo do prekinitev zvez, lahko pa zelo zmanjšaš učinke, ki jih prekinitve imajo na delovanje telekomunikacijskega sistema, posledično pa tudi na delovanje elektroenergetskega sistema.

LITERATURA

[1] Interno poročilo o odpravi posledic žledoloma

[2] Interna brošura Elektroenergetsko omrežje Slovenije z obratovalnimi podatki za leto 2014

Marija Mrzel-Ljubič je vodja službe za telekomunikacije in TK infrastrukturo v podjetju ELES, d.o.o.

mag. **Venčeslav Perko** je direktor področja za informatiko in telekomunikacije v podjetju ELES, d.o.o.

Goran Uršič je pomočnik vodje službe za telekomunikacije in TK infrastrukturo v podjetju ELES, d.o.o.

Nadzorni sistem kot ključni element učinkovite in zanesljive infrastrukture

Saša Sokolić in Aljaž Stare, Metronik, d. o. o., Ljubljana

Povzetek — V prispevku je obdelana problematika oddaljenega nadzora nad infrastrukturnimi objekti in elementi. Prikazani so tipični izzivi, potencialne težave in možne tehnične rešitve. Opisani so principi zajema, prikaza, shranjevanja in obdelave podatkov. Prikazani so konkretni primeri izvedbe in pridobitve za uporabnike.

Ključne besede — nadzorni sistemi, zajem podatkov, shranjevanje procesnih podatkov, procesni historian

Abstract — In this paper the general questions of remote control solutions of the infrastructure facilities are explained. Typical challenges, potential issues and possible technical solutions are discussed. The basic principles of data acquisition, visualization, data archiving and transformation are described. At the end concrete implementation examples are shown with the benefits for the end user.

Keywords — control systems, data aquisition, process data archiving, process historian

I. UVOD

V infrastrukturnih podjetjih se zaradi narave sistemov in procesov, ki jih upravljajo, soočajo s problemi kakovostnega oddaljenega nadzora in vodenja. Govorimo o sistemih, ki so geografsko razpršeni s ciljem zagotavljanja kritičnih javnih in komercialnih storitev, kot so npr. telekomunikacijski sistemi, sistemi preskrbe s pitno vodo, plinom ali električno energijo, železniški promet in drugi. V primeru informacijskih in telekomunikacijskih storitev so to telekomunikacijska omrežja s svojo strojno in programsko opremo (npr. bazne postaje mobilne telefonije, strežniška oprema, sistemi za klimatizacijo, brezprekinitveno napajanje ipd.). Kljub precejšnji avtonomnosti posameznih sistemov – tako funkcionalno kot tudi s stališča lokacije opreme, je za večjo zanesljivost, razpoložljivost in gospodarnost delovanja ter učinkovitejše vzdrževanje potrebna uvedba oddaljenega nadzornega sistema. Takšne sisteme, kjer se pojavlja potreba po izmenjavi podatkov med oddaljenimi lokacijami, v splošnem imenujemo tudi telemetrijski sistemi.

Kompleksni (telemetrijski) sistem za nadzor in oddaljeno upravljanje je v grobem sestavljen iz lokalnih naprav za zajem podatkov, komunikacijskega sistema za prenos podatkov in centralnega nadzornega sistema (CNS) s sistemom za arhiviranje in distribucijo procesnih podatkov – procesni historian. Tovrsten sistem omogoča vizualizacijo in upravljanje oddaljenih naprav ter napredno alarmiranje in analiziranje podatkov ter poročanje, kar lahko predstavlja tudi odlično osnovo za orodja za obvladovanje učinkovitosti, vzdrževanje, energetski management in kompleksnejša orodja za detekcijo napak in optimizacijo procesa.

Za izgradnjo tovrstnega sistema in izbiro primerne rešitve je potrebno skrbno preučiti opremo, ki bo predmet nadzora in upravljanja, kot tudi komunikacijsko infrastrukturo za prenos podatkov, ki je na razpolago, in definirati funkcionalnosti, ki jih želimo od takšnega nadzornega sistema. Izkušnje kažejo, da je pri tem izredno pomembno, da se izbirajo rešitve, ki so odprte, standardne in uveljavljene, s čimer se zagotovi trajnejša vrednost naložbe in enostavnejše vzdrževanje in nadgradnja.

V nadaljevanju bomo prikazali značilnosti in funkcije kompleksnega sistema za nadzor in oddaljeno upravljanje, parametre upravljanja, njegove gradnike in primer konkretne implementacije.

II. ZNAČILNOSTI IN FUNKCIJE KOMPLEKSNEGA NADZORNEGA SISTEMA

A. Komunikacijska infrastruktura

Pri postavitvi nadzornih sistemov se za prenos podatkov v praksi uporabljajo različni komunikacijski mediji. V zadnjem času so najpogosteje uporabljene naslednje možnosti:

- omrežja, ki temeljijo na Ethernet standardih,
- mobilna telekomunikacijska omrežja (npr. GSM),
- omrežja, ki temeljijo na lokalnih radijskih zvezah.

Vsaka od možnosti ima svoje značilnosti oziroma svoje prednosti in pomanjkljivosti. Mnogi nadzorni sistemi pa tudi kombinirajo več različnih prenosnih poti, kar omogoča večjo razpoložljivost sistemov.

Ethernet je po večini kriterijev dobra izbira. Vendar je lahko izgradnja Ethernet omrežja zelo zahtevna in cenovno neugodna. To velja posebej takrat, ko gre za nadzor majhnih objektov, ki se nahajajo izven urbanih področij. Za nadzor naprav preko Ethernet omrežja se pogosto uporablja SNMP (Simple Network Managment Protokol).

Začetna investicija je pri uporabi mobilnega omrežja v primerjavi z lastnim Ethernet omrežjem minimalna. So pa zato stroški obratovanja višji, saj je potrebno operaterju mobilnega omrežja plačevati za prenos podatkov. Z ustreznimi mehanizmi prenosa podatkov (več v nadaljevanju), lahko sicer količino prenesenih podatkov in s tem povezanih stroškov, bistveno zmanjšamo. V primeru GSM omrežja je možen tudi prenos podatkov preko vzpostavljanja klicnih povezav. V tem primeru operater zaračunava stroške glede na čas vzpostavljene zveze. Vendar je cenovno ta način precej neugoden. Dodatna pomanjkljivost tega načina je dolg čas vzpostavljanja zveze in omejeno število istočasnih povezav. Zato se ta način v praksi ne pojavlja pogosto. Javno GSM omrežje ima še eno pomanjkljivost, t. i. kritične aplikacije. V primeru izrednih dogodkov (potresi, poplave, nesreče, večji dogodki) lahko pride do preobremenjenosti omrežja in posledično izgube povezave med centrom vodenja in nadziranimi objekti. Za takšne primere mora telemetrijski sistem zagotoviti lokalno

shranjevanje podatkov (alarmi, dogodki). Ti se ob ponovni vzpostavitvi povezave prenesejo v center vodenja.

Sistem lastnih radijskih zvez je v veliko primerih dober kompromis za telemetrijske sisteme. Vendar je tudi v tem primeru začetna investicija višja kot pri uporabi GSM omrežja. Implementacija sistema je zahtevnejša, saj so prenosne hitrosti zaradi omejene širine radijskih kanalov manjše.

B. Načini prenosa podatkov v center vodenja

Najpogostejši način za zajem podatkov iz oddaljenih lokacij je ciklično povpraševanje po podatkih (polling). Običajno na ta način prenašamo trenutne podatke, za katere je alarmiranje izvedeno v centru vodenja. Glavna prednost tega načina je, da je enostaven za realizacijo. Primeren je predvsem za manjše in enostavne sisteme. Ker se v vsakem ciklu prenašajo vsi podatki iz vseh objektov, lahko to pri večjih sistemih privede do neažurnosti podatkov. Druga pomanjkljivost tega načina je, da spremembe, ki so krajše od časa, ki je potreben za obhod vseh objektov, nadzorni sistem ne zazna.

Druga možnost je dogodkovno proženje prenosa podatkov (t.i. »unsolicited messaging« način). V tem primeru mora biti na lokalni postaji izvedena logika, ki zaznava dogodke. Ob pojavu dogodka, se podatki prenesejo v center vodenja. Primeri dogodkov so spremembe merjenih veličin (npr. sprememba nivoja), alarmi (npr. okvara motorja) ali pa dogodki, ki so pogojeni z logiko delovanja objektov (npr. vklop črpalke). Princip dogodkovno proženega prenosa podatkov je ugoden s stališča količine prenesenih podatkov, vendar pa je realizacija in vzdrževanje sistema zahtevnejša od »polling« načina.

Tretja možnost za prenos podatkov je povezana z lokalnim arhiviranjem podatkov (t.i. »polled report by exception« način). V tem primeru se dogodki shranjujejo na oddaljeni lokaciji, kjer se opremijo s časovno značko trenutka, ko se je dogodek zgodil. Dogodki se prenesejo v center ciklično na osnovi »polling« načina. Prednost tega načina je, da se tipično v center prenaša manjše število podatkov in da tudi v primeru izpada povezave s centrom ne pride do izgube podatkov (dogodkov).

V praksi pogosto srečujemo kombinacije opisanih načinov za prenos podatkov v center vodenja.

C. Izbira protokola

Pomemben člen pri izgradnji nadzornega sistema je tudi uporabljen protokol, ki predstavlja jezik za izmenjavo sporočil po fizičnem komunikacijskem mediju. Možnosti je zelo veliko. Treba pa se je zavedati, da je izbira protokola močno odvisna tudi od izbranega komunikacijska medija in samih naprav, ki jih povezujemo. Od standardih protokolov najpogostejše srečujemo naslednje protokole:

- Modbus
- SNMP
- DNP3 (IEC 60870-5)

Modbus protokol je brez dvoma najbolj razširjen protokol v industrijski avtomatizaciji. Svoje mesto je našel tudi v telemetrijskih sistemih. Glavni razlogi za to so njegova enostavnost, razširjenost in učinkovitost. Modbus protokol je primeren samo za »polling« način delovanja, saj deluje po principu master(sprašuje)/slave(odgovarja). Osnovni protokol ne podpira prenosa podatkov opremljenih s časovno značko.

SNMP (Simple Networking Managment Protocol) se predvsem uporablja pri nadzoru komunikacijskih in IT naprav. Za razliko od Modbus protokola SNMP podpira tudi dogodkovno proženo pošiljanje podatkov na nadzorni računalnik. V SNMP terminologiji jih imenujemo »Trap«. SNMP protokol ne podpira podatkov, opremljenih s časovno značko.

DNP3 in IEC 60870-5 sta v osnovi zelo podobna protokola saj je bil njun razvoj povezan. To sta protokola, ki sta bila namensko razvita za potrebe telemetrije in zato sistemsko podpirata vse principe, ki se v telemetrijskih sistemih danes uporabljajo. Razlog, da se protokola v praksi ne uporabljata bolj masovno, je v njuni kompleksnosti in zato tudi dragi implementaciji.

D. Nadzorni sistem

Ključni element za zagotovitev zanesljive in učinkovite infrastrukture prestavlja nadzorni sistem, ki omogoča vizualizacijo sistemov in upravljanje z oddaljenimi napravami (npr. vklop/izklop klime, nastavitev parametrov delovanja,…), alarmiranje in obveščanje na daljavo preko SMS sporočil ali elektronske pošte, diagnostiko napak za hitro ukrepanje, izdelavo poročil itd.

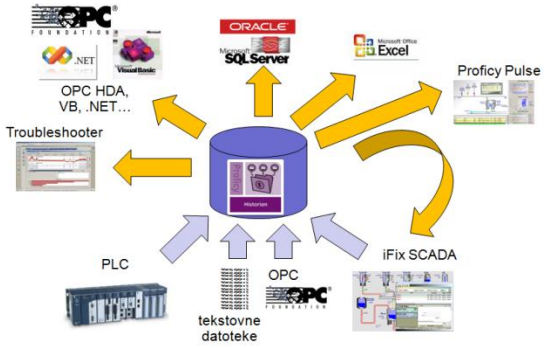
Pri izbiri nadzornega sistema moramo biti zelo pazljivi, saj mora le-ta biti dovolj odprt, da lahko preko različnih protokolov (npr. Modbus, SNMP, DNP3, itd.) povezujemo različne (komunikacijske in IT) naprave in vse te informacije posredujemo različnim drugim aplikacijam. Poleg tega mora biti nadzorni sistem dovolj robusten (redundanca), predvsem s stališča vzdrževanja geografsko distribuiranega sistema pa je koristno tudi, če omogoča pregled in/ali upravljanje z mobilnih naprav.

Na trgu obstajajo razni namenski nadzorni sistemi, ki so bili razviti posebno za nadzor infrastrukture (npr. HP OpenView – HP BTO, IBM Tivoli, itd.). Po drugi strani pa obstaja vrsta splošno namenskih rešitev, ki se že vrsto let uspešno uporabljajo v raznih tipih industrije. Takšne rešitve so v osnovi zelo odprte in funkcionalne, kjer je možno vključevati raznovrstne želje uporabnikov (animacije, topološki/organizacijski model različnih sistemov, poročila,…). Prednost takšnih splošno namenskih rešitev, v primerjavi z namenskimi nadzornimi sistemi, je tudi nižja cena in široka baza sistemskih integratorjev, ki so sposobni skrbeti za sistem, ga vzdrževati, nadgrajevati in širiti. S tem končni uporabnik ni vezan le na eno ekipo izvajalcev, ki so sposobni obvladovati takšen nadzorni sistem. Zaradi tega je danes čedalje manj pravih razlogov, zakaj bi podjetja posegala po dragih namenskih orodjih za nadzor infrastukture, z majhnim naborom podjetij na slovenskem trgu, ki so sposobni obvladovati takšne kompleksne sisteme.

E. Učinkovit arhiv in analiza procesnih podatkov

Z namenom izboljšanja vizualizacije procesov, produktivnosti, učinkovitosti, optimizacije stroškov itd. je ključnega pomena, da zaposleni v podjetjih (npr. operaterji, inženirji, managerji, itd.) hitro prihajajo do pravih informacij v realnem času in dobijo kakovosten vpogled v delovanje celotnega sistema z enega mesta. Zato je bistveno, da vse procesne podatke, ki so pomembni s stališča upravljanja, delovanja, vzdrževanja in ostalih inženirskih funkcij,

integriramo v enoten sistem. Takšen sistem mora tako različnim profilom uporabnikov omogočati hiter in enostaven način pregledovanja, analiziranja in primerjave procesnih podatkov, po drugi strani pa mora biti sposoben tudi posredovanja teh podatkov različnim proizvodnim in poslovnim informacijskim sistemom.

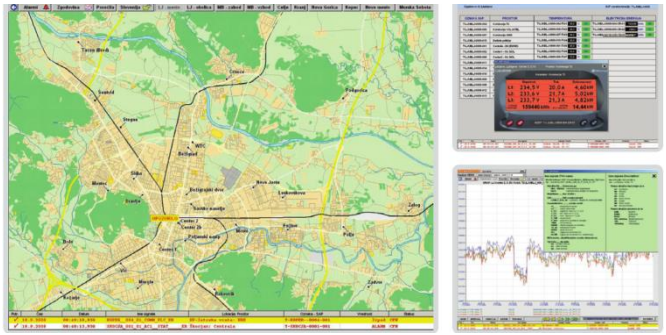


Slika 1: Arhitektura na osnovi procesnega historiana

S tem namenom se v večini primerov koristi procesni historian, ki je sposoben učinkovito zbirati ogromno količino procesnih podatkov iz različnih virov (SCADA, PLC, datotek) in pri tem izvajati močno kompresijo podatkov, po drugi strani pa je sposoben posredovati podatke množici različnih tipov odjemalcev (Excel, Web, SCADA, relacijske baze,…).

III. PRIMER TELEKOMA SLOVENIJE

Telekom Slovenije ima razpredene postaje s telekomunikacijsko opremo po celotnem območju Slovenije. Za nemoteno delovanje le-te je potrebno zagotavljati kakovostno električno energijo in ustrezne klimatske pogoje; kar pa zahteva stalno spremljanje in nadzor delovanja vseh elektroenergetskih in klima sistemov ter okoljskih parametrov. To pa je težko doseči brez ustreznega računalniškega sistema, ki omogoča daljinski nadzor. S tem namenom je Telekom Slovenije, skupaj s podjetjem Metronik, izvedel projekt postavitve centralnega telemetrijskega sistema CNEEKS za daljinsko zbiranje ključnih podatkov iz vseh postaj in podporo operaterju pri izvajanju nadzora. Na zasnovo sistema CNEEKS je pomembno vplivala zahteva Telekoma, da mora biti centralni nadzorni sistem povezan s krovnim nadzornim sistemom TeMIP ter mora omogočati nadaljnjo širitev telekomunikacijske mreže. Zagotavljati mora predvsem enostavno vključevanje novih naprav, senzorjev in novih postaj v sistem.



Slika 2: Primer slik nadzornega sistema v Telekomu Slovenije

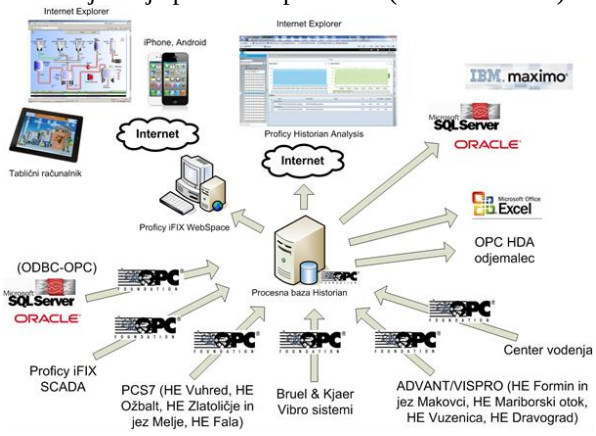
Z Metronikovim sistemom daljinskega nadzora so pooblaščeni vzdrževalci Telekoma dobili orodje, s katerim lahko na učinkovit in racionalen način nadzorujejo ključne parametre elektroenergetskih in klima sistemov na vseh lokacijah po Sloveniji. Omogoča jim sprotno spremljanje delovanja in pravočasno odkrivanje dogodkov, ki lahko pripeljejo do izpadov na telekomunikacijskem omrežju.

Telekom je na tak način povečal varnost in zanesljivost delovanja svoje infrastrukture, kar posledično pomeni višjo raven kakovosti storitev za končne uporabnike telekomunikacijskega omrežja. Uporaba sistema CNEEKS jamči nižje stroške obratovanja in vzdrževanja. Poleg tega pa sproten nadzor nad porabljeno energijo pripomore tudi k energetski varčnosti in racionalizaciji stroškov ter k boljšemu vrednotenju porabljene energije. In nenazadnje; Telekom je dobil tehnološko sodoben telemetrijski sistem, ki lahko sledi razvojni strategiji podjetja in širitvi telekomunikacijske infrastrukture.

IV. PRIMER DRAVSKIH ELEKTRARN MARIBOR

Družba Dravske elektrarne Maribor d.o.o. (DEM) je največji proizvajalec električne energije iz obnovljivih virov v Sloveniji. Z osmimi hidroelektrarnami na reki Dravi, s tremi malimi hidroelektrarnami in štirimi sončnimi elektrarnami proizvedejo kar 23 % električne energije v Sloveniji. To predstavlja 80 odstotkov slovenske električne energije, ki ustreza kriterijem obnovljivih virov in standardom mednarodno priznanega certifikata RECS (Renewable Energy Certificates System). Kakovostno energijo zagotavljajo na okolju prijazen način in s spoštovanjem načel trajnostnega razvoja

V podjetju DEM so se kot uporabniki procesnih sistemov Siemens PCS7, ABB ADVANT/VISPRO, Proficy iFIX SCADA, SQL, Bruel & Kjaer Vibro sistemi ter Center vodenja v letu 2013 odločili za vzpostavitev naprednega sistema za zajemanje, vrednotenje, analiziranje, predstavitev in shranjevanje procesnih podatkov (sistem ZVAPS).



Slika 3: Arhitektura sistema na Dravskih elektrarnah Maribor

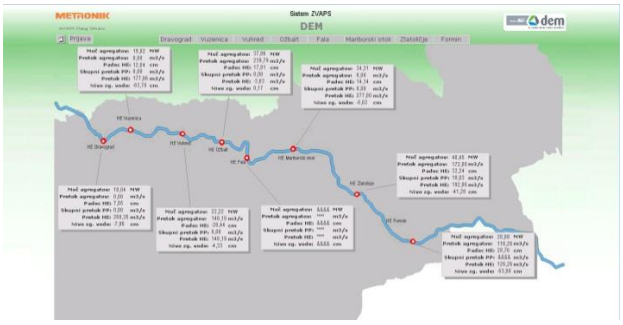
Sistem ZVAPS temelji na uporabi treh gradnikov (programskih orodjih) proizvajalca programske opreme General Electric Intelligent Platforms:

– specializirana centralna podatkovna baza za shranjevanje procesnih podatkov (Proficy Historian),

- programsko orodje za izdelavo procesnih slik in dostop do le-teh preko spletnega brskalnika (Proficy iFIX WebSpace),
- namensko programsko orodje za grafično analizo procesnih podatkov, do katerih lahko uporabniki dostopajo preko spletnega brskalnika (Proficy Historian Analysis.

Z Metronikovo rešitvijo so Dravske elektrarne Maribor pridobile sodoben, zanesljiv in uporaben sistem za zajemanje, vrednotenje, analiziranje, predstavitev in shranjevanje procesnih podatkov. Sistem Dravskim elektrarnam prinaša:

- sistematično ureditev arhiva procesnih podatkov. Naročnik je dobil varen, siguren in lahko dostopen arhiv procesnih podatkov, ki omogoča naprednejšo analizo meritev in drugih procesnih veličin;
- omogočen enostaven dostop ter izmenjava procesnih podatkov z drugimi sistemi in s tem olajšano sodelovanje med različnimi službami s ciljem izboljšanja učinkovitosti in varnosti;
- skupen vpogled v sisteme vodenja z izrazito ločitvijo od funkcij upravljanja;
- možnost izdelovanja kompleksnih grafičnih prikazov in izdelovanja poljubnih procesnih slik in gradnikov;
- nižje stroške izdelave obsežnih in uporabniku prilagojenih operativnih poročil. Ta se izdelajo že v okviru Microsoft Excel orodja, brez potrebe po posebnem razvoju takšnih poročil in poseganja v nadzorni (SCADA) sistem ali sekundarno opremo.



Slika 4: Prikaz informacij preko spletnega brskalnika z uporabo Proficy WebSpace.

Slika 5: Grafični prikaz podatkov znotraj internetnega brskalnika z uporabo Proficy Historian Analysis

V. KAKO SE LOTITI INVESTICIJE IN IZBRATI OPREMO

Z vidika izvedbe oz. izbire rešitve se vse bolj uveljavlja pristop, ki temelji na uporabi standardnih orodij in tehnologij. Kot primer naj navedemo dejstvo, da Gartner Group, vodilno podjetje za svetovanje na področji IT tehnologij in razvoja, svojim partnerjem in strankam priporoča zmanjševanje namenske kode in programov. Zato tudi ne preseneča dejstvo, da večina uspešnih podjetij v Sloveniji in svetu posega po opremi in tehnologiji z naslednjimi lastnostmi:

- Oprema/tehnologija ima v lokalnem in globalnem okolju dovolj močno podporo in je ne uporablja/razvija samo en sistemski integrator, s čimer naročnik ni odvisen le od enega izvajalca, ki lahko v nekaj letih izgine s trga,
- Oprema/tehnologija zagotavlja morebitne nadgradnje in širitve, brez večjih posegov in s tem povezanih dodatnih del,
- Opremo/tehnologijo lahko s standardnimi rešitvami povežemo z informacijskimi in drugimi sistemi podjetja,
- Oprema/tehnologija je uveljavljena in odprta (za razliko od »nestandardnih« in namenskih rešitev), ter uporabniku omogoča, da rešitev vzdržuje/nadgrajuje sam ali z drugimi partnerji, kar zagotavlja dolgoročno varnost investicije,
- Oprema/tehnologija sledi novim smernicam (npr. mobilne naprave, podpora operacijskim sistemom, standardnim vmesnikom in protokolom).
- Rešitev je možno zlahka nadgraditi z naprednejšimi funkcijami kot so napredna analitika, napovedovanje ali napredna diagnostika napak.

VI. ZAKLJUČEK

Na trgu že dolgo obstaja potreba po oddaljenih nadzornih sistemih, saj z njimi zagotavljamo večjo razpoložljivost nadziranih sistemov in njihovo gospodarno delovanje. Čedalje bolj pa se kaže tudi potreba po nadzoru sistemov na področjih, ki so se v zadnjih letih najbolj razvila (npr. bazne postaje mobilnega telefonskega omrežja, naprave za brezžični prenos podatkov, nadzor delovanja UPS-sistemov itd.). Pri gradnji takšnih sistemov se skriva veliko pasti, na katere je treba biti posebno pozoren in jih temeljito preučiti.

Za realizacijo posameznih sklopov nadzornega sistema je na razpolago več rešitev. V večini primerov pa se izkaže, da je s stališča dolgoročne uporabnosti sistema in varnosti investicije, najbolje rešitev zasnovati na uporabi standardnih orodij in tehnologij, brez posebno razvite namenske kode in programov. Tako lahko rešitev vzdržuje, nadgrajuje in širi uporabnik sam, ali pa z drugimi partnerji, brez večjih posegov in s tem povezanih dodatnih stroškov.

Saša Sokolić je diplomiral, magistriral in doktoriral na Fakulteti za elektrotehniko v Ljubljani v letih 1989, 1992 in 1996. Od leta 1996 je zaposlen v podjetju Metronik, kjer je kot član uprave odgovoren za marketing in prodajo, obenem pa v okviru podjetja vodi tudi razvojno skupino. Njegovo strokovno delo je osredotočeno na proizvodne informacijske sisteme in na sodobne tehnologije procesnega vodenja, sodeluje pa tudi pri uvajanju tovrstnih rešitev v vodilna slovenska podjetja. Saša Sokolić je avtor številnih znanstvenih člankov in prispevkov na znanstvenih in strokovnih posvetovanjih, objavil pa je tudi veliko poljudno-strokovnih prispevkov s področja svojega dela.

Aljaž Stare je diplomiral leta 2002 in doktoriral leta 2007, oboje na Fakulteti za elektrotehniko Univerze v Ljubljani. Od leta 2008 je zaposlen v podjetju Metronik, kot vodja programa GE Intelligent Platforms. V okviru svojega dela se ukvarja z uvajanjem sodobnih tehnologij in rešitev na področje avtomatike in proizvodne informatike. Aljaž Stare je leta 2009 prejel tudi Zoisovo priznanje za pomembne dosežke na področju vodenja sistemov, ki ga podeljuje Ministrstvo za izobraževanje, znanost in šport.

Private vs. Public Critical Communications

Rade Maljevic, Kapsch CarrierCom AG, Vienna, Austria

Abstract — This article explains the fundamentals of private and public communication networks for mission critical use cases in public safety and transport, railways and power utilities smart grids. The focus is on the most relevant critical communications standards GSM-R and TETRA and how Kapsch is applying them in mission critical network environments.

Keywords — TETRA, GSM-R, Critical Communications, Kapsch, Public Transport, Railways, Utilities, Smart Grids

I. INTRODUCTION

Kapsch CarrierCom (KCC) is a global systems integrator and innovator that supplies fixed mobile, transportation and access network solutions. The 1892 founded and family owned Kapsch Group headquartered in Vienna is operating globally in 44 countries with 5.500 employees as a leader in the development of mission critical technologies for railways, public transport and carriers, including GSM-R digital wireless train communication. This is a field in which KCC is the market leader with 52% worldwide market share (based on contracted length of tracks). As a long-standing and key partner of railway and public transport operators, Kapsch has developed unique design and optimization radio expertise for both critical voice and ERTMS applications. This includes radio design and planning, coverage validation and optimisation services and also tunnel radio coverage. The corporation can rely on 30 years' experience in the critical communications business, and is consequently able to react quickly and with the required flexibility to meet any mission critical demands. The reference customers include some of the largest critical communications networks such as Deutsche Bahn, Network Rail UK and Réseau ferré de France as well as a number of network in urban public transport like Tyne & Wear Metro in Newcastle (UK) and Metro Rio de Janeiro.

II. CRITICAL COMMUNICATIONS NETWORKS

Critical Communications Networks are created specifically for public safety organisations as well as the public transport sector, which includes bus, tram, metro, railway and airport ground operations. Unlike commercial networks designed for the general public, a critical communications Network will provide the information security and reliability that responders require, especially during a crisis. Public safety and transport users simply can't afford to be without communications – their network must be an 'always available' lifeline to keep them in contact and up-to-date with vital information. Furthermore, the use of encryption to protect the security of voice or data messages throughout the critical communications network is vital to avoid compromising operational activities, to maintain safety and to keep the identity of users secret.

III. GSM-R AND TETRA

ETSI is the leading standards body developing open industry standards in communications. It has four digital mobile radio standards (TETRA, GSM/GSM-R, DMR, dPMR) and each of them started life with specific target markets and user requirements to meet. Two of them are specifically designed for the critical communications requirements: TETRA and GSM-R. But there is a degree of cross-over between the standards and in some areas this has led to certain competition.

GSM-R was developed specifically for the rail market following a decision in Europe in 1993 to agree the correct solution for European railways – TETRA came second. GSM-R focuses on safety, reliability, prevention of accidents, and emergency communication solely in the specific, and very specialised, domain of the rail industry. It has a big success across Europe, Asia and Africa. And there is currently significant developments in the rest of the world. Interoperability between manufacturers of equipment is a key requirement in maintaining a competitive landscape.

The major reason to go for TETRA is that it is more frequency efficient than other technologies and it provides excellent quality voice functionality and the ability to support mission-critical data services both highly encrypted and secured against cyber vulnerabilities. According to estimates by the TCCA [1] the majority of urban transport operators today will specify TETRA as best meeting its operational, safety and security requirements. In fact, although large-scale public safety projects drove TETRA's early applications development, the transportation sector has now overtaken the public safety market in terms of the number of individual networks deployed around the world. Some of the unique TETRA features which makes it a perfect fit for critical communications networks include:

- Multi-Organisation Network,
- Fast Call Setup,
- Busy queuing,
- Group Communication,
- Broadcast channels,
- Full and semi-duplex calls (push-to-talk operation),
- Support of direct mode in emergency cases where a network is not accessible (e.g. in tunnel rescue cases)
- Dynamic Group Number Assignment (DGNA),
- Priorities and Pre-Emptive Priorities; Emergency Call,
- Uncompromised Security and Air+E2E Encryption and Authentication,
- High Reliability and Availability,
- Comprehensive data services including Short Data Service (SDS); circuit mode data; Packet Data Service (PDS); multi-slot packet data and status messages.

Furthermore TETRA leads the way in managing an open standard through transparent interoperability certification: The majority of TETRA networks have a mix of supplier equipment. This competition in the TETRA industry has

enabled rapid progress in developing subscriber equipment, hand-portables and accessories and ensures competitive pricing.

IV. PRIVATE VS. PUBLIC NETWORKS

Unlike the GSM network the GSM-R and TETRA networks are private networks which means that they:

- have separate infrastructure,
- have separate base stations, and
- can be integrated with public networks.

Features and functionality aside the challenges for public cellular networks in supporting mission critical communications are that during disasters and major incidents:

- Call set-up times are not yet acceptable for professional mobile radio communications.
- Public Mobile Networks struggle to survive and often fail
- Infrastructure may be critically damaged, at best limiting service.
- It is extremely difficult, and often impractical, to prioritise calls and signalling to guarantee access to specific user types.
- Interoperability necessary between public safety agencies cannot rely on public networks.

	TETRA	GSM/UMTS
Call setup time (individual & group call)	0,5 sec	3-5 sec
Emergency call setup time	0,5 sec	2 sec
Call queuing	YES	NO
Late Entry	YES	NO
Transport	full IP	E1/IP
Frequency bands	380-430/450-470/806-866	900/1800/2100
Typical Cell Size	**15-25Km** radius	**5-15Km** radius

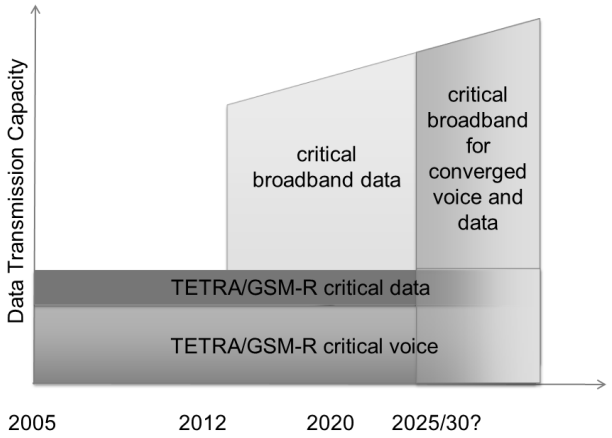
Picture 5: Private v. Public features / time performance comparison

Even though public cellular systems like UMTS and LTE cannot provide mission-critical communications but may have a role for additional not-critical data applications because of their faster data rates. However the link needs to be encrypted, if data security is important and therefore the device also needs to be considered when determining security requirements.

Identifying key requirements for a critical communication network will quickly develop a technology short list on what organizations want to achieve. This list is generally includes the topics of spectrum & regulatory approval, coverage and capacity, security, interoperability, resiliency, set-to-set operation (like the TETRA direct mode), multi-vendor questions, voice requirements, data requirements and not to forget to support control room applications (i.e. dispatch).

V. FUTURE OF CRITICAL COMMUNICATION

Since beginning LTE is fuelling the debate between using public networks for broadband data and implementing stand-alone private networks that support TETRA as an application to facilitate voice and broadband data. The most comprehensive approach is designed by the SALUS project [3] addressing the security and interoperability in next generation Public Protection and Disaster Relief (PPDR) communication infrastructures. However there is still a significant number of topics to be addressed in order to design LTE for critical applications (LTE-C) Current trunking LTE prototype trials are promising but all of them are not based on solid international standards which has an will always be a mandatory cornerstone of any future critical communications solution. Therefore TETRA and GSM-R are and will remain for some time the only standardized and productized technologies for critical communications networks. Consequently a hybrid approach by splitting application into critical private and minor critical public broadband requirements is assumed to be most likely a reasonable way forward to address today's business needs.



Picture 2: Private vs. Critical Communications Broadband Timeline

VI. PUBLIC TRANSPORT RUNS ON TETRA

The resilient, highly secure and performance of TETRA data services has turned out to be a key differentiator of this standard in the domain of public transport. To understand the true value of TETRA data services may not be assessed from the broadband but rather from the signalling perspective which is key to any operations in public transport. And the unique TETRA capability of the use of multiple secondary control channels to maintain short data throughput is of great value regarding data signalling applications for metro, tram, light rail and bus public transport operators (PTO).

Applications are successfully managing hundred millions of passenger journeys on all modes of public transport across the world. Some of the use cases are location information to manage vehicle flow, exchange of Intermodal Transport Control System data (ITCS builds the operational core application of a PTO), traffic management and SCADA signalling like traffic light control, vehicle sensors reporting like fuel and engine health and also real-time passenger information (RTPI)

In a metro, tram and light-rail operation the resilient TETRA data applications can be used in combination with RFID tags for automatic location tracking and talk group selection. In this application a vehicle receives address of RFID token in track and the position (tag ID) reported via TETRA network and appropriate talk group for location selected automatically

At airport TETRA is an enabler for improving logistics efficiency. As an example this capability is used by at a number of airports for automatic assignment of the flight numbers to become the name of the user talk group. In this use case the required resources to process a flight are dynamically assigned to a talk group which significantly

improves workflow, task reporting, airport information and other process related tasks.

The end-to-end TETRA solution of Kapsch based on innovative European TETRA technology is dedicated to supplying comprehensive and secure radio communications infrastructure to mission and business-critical environments. The company's longstanding experience with critical telecommunications systems and the leading technology provided by Kapsch were the main factors that resulted in the latest major contract wins. This mission critical communications networks based on the TETRA standard are for the UK´s 2nd largest subway networks at the Tyne & Wear Metro in Newcastle and the Metro Rio de Janeiro expansion to support the Olympic Games 2016.

VII. TRAINS OPERATED WITH ETCS (EUROPEAN TRAIN CONTROL SYSTEM) BASED ON GSM-R

Railways operate in a competitive environment and have to ensure operational safety, international interoperability, growth of transport capacities, and the reduction of travel time and reduction of life-cycle costs for equipment. European railways had to deal with more than six different types of railway electrification and about 20 different train control-command systems which complex and costly especially for border crossing traffic. To bear with the high cost of the different signalling and communication systems, the European Commission supported the definition of GSM for Railways (GSM-R) as the new digital radio system for railway internal voice and data communication, and the European Train Control System (ETCS) as the new control & command system.

The combination of ETCS and GSM-R form a new signalling and critical communication system, the European Railway Traffic Management System (ERTMS). GSM-R is part of the ERTMS standard and carries the signalling information directly to the train on-board signalling unit, enabling higher train speeds and traffic density with a high level of safety.

GSM-R is based on public GSM and provides a rich set of critical communications features addressing the specific needs of railway operators. Examples of advanced features are group calls, voice broadcast, location based connections, and call pre-emption in case of an emergency.

GSM-R provides a secure critical communications platform for voice and data communication between the operational staff of the railway companies including drivers, dispatchers, shunting team members, train engineers, and station controllers.

The latest ETCS Level 3 has an on-board train integrity system which monitors the train. There is no requirement for train detection equipment. The solution relies on a critical communications an on-board GSM-R radio communication system to allow the on- board computer communication with the control centre and electronic balises as kilometre markers.

Kapsch's outstanding experience in critical communications GSM-R services and technology make the company the leading global provider for GSM based radio communication to railway networks. Kapsch has been awarded the largest GSM-R networks in Europe, Africa and Asia covering the major part of railway tracks among the over 75,000 km deploy GSM-R networks, including national contracts in Germany, France, UK, Austria and many others. Some of the latest projects additions currently deployed are national railway networks of Hungary and Slovenia.

VIII. UTILITIES SMART GRIDS RELY ON CRITICAL COMMUNICATION

Critical communication for utilities is becoming increasingly important as Smart Grids develop. According to the EUTC position paper [2] communication services are already necessary for mission-critical utility grid. The European Utility Telecom Council recommends a dedicated spectrum for utilities in the UHF frequency range (450-470 MHz) to satisfy strategic and the technical conditions for the roll-out of smart meters as well as for grid management. The main reason for this recommendation is that the geographical coverage offered in this frequency range is optimal and also this band supports many standardised and proven mass-market technologies which will bring cost benefits to consumers and lower the risk associated with new or customised technologies.

TETRA technologies provide ideal solutions because they are standards-based and extremely secure and robust against cyber vulnerability. They provide coverage and levels of availability that commercial wireless networks cannot match. Furthermore despite unfounded rumours TETRA provides sufficient bandwidth for smart control of electric energy distribution. In addition with the large area coverage capabilities and embedded integration with other communication systems traditionally in use in utility companies the TETRA standard is an ideal setup for Smart Grid environment.

Providing a high level of security is essential for energy utility companies since any outages of critical power infrastructure represents a severe threat to our society and from a commercial point of view reduces business profitability. Energy networks must therefore be robust and protected against threats such as technical problems, natural disasters and targeted attacks. Countering the threat of cybercrime is an increasingly high priority for energy companies.

Using the TETRA radio networks increases the overall security, reliability and integrity of a SCADA communications solution, even when using commercial data communications. Commercial wireless networks may support higher data bandwidth than TETRA but they are not even coming close to the unprecedented reliably and security of TETRA data. The TETRA communication achieves data security, integrity and priority control over several communications networks, with immunity to virus infections and network attacks such as Denial of Service when using commercial wireless networks. Early detection of communications channel problems is another advantage, while also being insulated from Internet system incidents

An essential element of Smart Grids is a secure and reliable communications network that connects the various energy network's components like power stations, transmission network, network and most important the endpoint meter facilities. In this scenario the communications network is required to act as an backbone network, helping to control and monitor the power grid and its components.

Power utilities use a TETRA network as a mission critical transport layer for electricity network control and monitoring applications. These include remote meter reading, direct load control systems, power distribution automation, monitoring wind speed on transmission lines, undersea power cable monitoring and transformer monitoring.

The tight integration with operational applications is a key factor for any utility since they use various systems to monitor and control their power networks. Information gathered from the power grid and delivered via the TETRA network is therefore combined into existing SCADA and control systems. Integration is needed for existing electricity network elements such as substations, breakers and transformers. Either serial as well as IP-based protocols are communicated by TETRA data devices. For the data communication via a TETRA infrastructure the utility can choose between SDS-based or Packet Data transfer. Energy utilities in Europe use common standards IEC 60870-5-101 or IEC 60870-5-104. In Asia and the U.S. they generally use the Modbus RTU or DNP3 protocol. In addition to the serial asynchronous protocols, TETRA is also capable to process UDP- and TCP-protocols. In this case, the data device operates as a TETRA router.

Kapsch provided critical communications solution for utilities that incorporates a TETRA digital radio system, SCADA gateways and RTU interface units meets all these needs to ensure functional and operational requirements, and also the safety and security.

ACKNOWLEDGMENTS

This article was supported by contributions of Thomas Putz the Solution Manager for Public Transport at Kapsch CarrierCom. This section includes the acknowledgments to those people and organizations that have contributed to the preparation of the paper. Here we would like to kindly acknowledge all the previous authors of this document.

LITERATURE

[1] Eurotransport Magazine, 2014, Robin Davis http://www.eurotransportmagazine.com/advent-calendar/why-tetra/

[2] EUTC position paper „Spectrum needs for Utilities", Issue 1.0, 2013 http://eutc.org/system/files/UTC_private_file/EUTC%20Spectrum%20Position%20Paper-9April2013.pdf

[3] SALUS project "Security and interoperability in next generation Public Protection and Disaster Relief (PPDR) communication infrastructure" https://www.sec-salus.eu/

Rade Maljević was born in 1973 in Sarajevo, BiH. He graduated at Faculty of Electrical Engineering, Univesity of Novi Sad in 1999. Currently, Rade is head of critical communication for public transport at Kapsch CarrierCom AG, Vienna, Austria. He started his career at Telekom Srpske, BiH as radio team manager in 1999. From 2001 to 2006 he was technical consultant for GSM and UTRAN products and solutions and from 2006 to 2008 he was account manager, both at Siemens AG Austria. From 2008 to 2012 he was sales manager at Nokia Siemens Networks in Austria. In 2012 he moved to Kapsch CarrierCom AG as sales manager PMR.

Postavitev in optimizacija brezžičnih mobilnih omrežij v izrednih razmerah

Andrej Vilhar, Andrej Hrovat in Tomaž Javornik, Inštitut Jožef Stefan, Ljubljana, Slovenija

Povzetek — V izrednih razmerah, kot so naravne nesreče večjih razsežnosti, je bistvenega pomena hitra in učinkovita vzpostavitev začasnega brezžičnega mobilnega omrežja, namenjenega nujnim komunikacijam in prenosu informacij. Arhitekturo začasnih mobilnih omrežij, namenjenih komunikacijam v izrednih razmerah, ki je predlagana v evropskem projektu ABSOLUTE, sestavljajo prenosne zemeljske bazne postaje ter prenosne zračne bazne postaje, nameščene na posebnih zračnih plovilih, lebdečih nekaj sto metrov nad tlemi (low altitude platform, LAP), ki so kombinacija balona in zmaja. Z bazno postajo, nameščeno na zračno plovilo, zagotovimo široko pokritost terena, medtem ko zemeljske postaje zagotavljajo zahtevano kapaciteto radijskega omrežja. Optimizacija parametrov opisanega celičnega omrežja pa ni enostavna zaradi interferenčnih motenj, ki jih povzroča radijska celica, nameščena na zračni ploščadi. V članku predlagamo metodo optimizacije začasnega omrežja LTE za namene komuniciranja v izrednih razmerah. Predlagana rešitev vsebuje radijsko planiranje, izvedeno z uporabo odprtokodnega orodja GRASS-RaPlaT razvitega na Inštitutu Jožef Stefan in optimizacijo parametrov omrežja z uporabo večkriterijskega evolucijskega algoritma. Lastnosti postavljenega začasnega mobilnega omrežja so odvisne od načrtovanih in natančno določenih lokacij, višin anten in oddajnih moči baznih postaj. Cilj optimizacije je določitev optimalne arhitekture mobilnega omrežja za izredne razmere, pri kateri bo pokritost ogroženega območja maksimalna, minimalna interferenca med posameznimi celicami in čim višja kapaciteta povezav. V prispevku bomo prikazali dva scenarija, in sicer: (i) soobstoj arhitekture za komunikacije v izrednih razmerah z obstoječim komercialnim mobilnim omrežjem in (ii) upravljanje topologije baznih postaj, ki je sestavljena iz zračnih (AeNB) in zemeljskih (PLMU) baznih postaj.

Ključne besede — arhitektura mobilnega omrežja, izredne razmere, optimizacija, kriterijske funkcije, evolucijski algoritem, GRASS-RaPlaT

Abstract — In the emergency situations such as extensive natural disasters the rapid and effective establishment of temporary wireless mobile network for emergency communications and transmission of information is essential. Architecture of temporary mobile network for communications in emergency situations, proposed by European project ABSOLUTE, consists of portable land mobile base stations and mobile aerial base station embedded in Low Altitude Platforms (LAPs), which are a combination of balloon and kite (helikite). Base stations installed on the aircrafts provide broad terrain coverage, while earth stations deliver the required capacity of the radio network. Due to interference caused by radio cell mounted on the aerial platforms the optimization of the described cellular network is a challenging task. In this paper we propose a method to optimize temporary LTE network for the communications in emergency situations. The proposed solution consists of radio planning carried out by open source tools GRASS-RaPlaT developed at the "Jozef Stefan" Institute and network parameters optimization using multi-objective evolutionary algorithm. Properties of the temporary mobile network depend on the accurate planning of the specified locations, base stations antenna height and transmit power. The optimization objective is to determine the optimal architecture of the mobile network for emergency situations with the maximal coverage of the affected area, lowest interference between cells and the maximum links capacity. In this paper we analyze two scenarios, namely (i) the coexistence of architecture for communications in emergency situations with the existing commercial cellular network and (ii) topology management of the base stations, which consists of aerial (AeNB) and earth (PLMU) base stations.

Keywords — mobile network architecture, emergency situations, optimization, criteria functions, evolutionary algorithm, GRASS-RaPlaT

I. UVOD

Optimizacija mobilnih omrežij je iterativni postopek sestavljen iz več korakov, katerega cilj je doseči maksimalno učinkovitost omrežja. Ena od ključnih točk je optimizacija lokacij baznih postaj (BS), na kar vplivajo številni faktorji. Poleg dejstva, da je število možnih lokacij za postavitev baznih postaj pogosto omejeno zaradi pravnih razlogov, se, zlasti v izrednih razmerah, pogosto dogodi, da postavitev na določeno lokacijo ni fizično izvedljiva (lokacija prenevarna, nedostopna, itd.). Postavitev baznih postaj običajno poteka v dveh korakih. V prvem koraku nameščene bazne postaje zagotavljajo pokritost področja s signalom nad določeno mejno vrednostjo. V drugem koraku pa je treba za zagotovitev ustrezne kapacitete omrežja na izbranih področjih izvesti zgoščevanje omrežja. Nadaljnje izboljšanje učinkovitost sistema je možno doseči s prilagajanjem nastavitev baznih postaj.

Algoritmi za postavitev baznih postaj ter za izboljšanje pokritja in kapacitete omrežja že obstajajo [1, 2]. Vendar pa problematika optimizacije LTE in LTE-Advanced sistemov z realnimi podatki o profilu terenu in podatkov o zgradbah ter uporabo najnovejših orodij za načrtovanje omrežij še ni bila natančneje obdelana. Poleg tega pa je, v smislu izrednih scenarijev, popolnoma zanemarjena tudi analiza soobstoja preživele komercialne komunikacijske infrastrukture in oportunističnih baznih postaj. Zato smo razvili nov optimizacijski postopek, ki temelji na odprtokodnem RF planerskem orodju GRASS RaPlaT [3] in evolucijskem algoritmu (EA) AMS-DEMO [4].

Cilj predlagane rešitve je povečanje učinkovitosti omrežja, zmanjšanje potrebnih virov in posledično zmanjšanje stroškov obratovanja. Na osnovi profila terena, podatkov o zgradbah in z uporabo najnovejših statističnih modelov orodje izračuna izgubo poti in z maksimiranjem izbranih kriterijskih funkcij določi optimalne lokacije in parametre baznih postaj. Orodje je popolnoma generično in je ob ustrezni izbiri kriterijskih funkcij uporabno za načrtovanje kateregakoli brezžičnega mobilnega omrežja.

Razvito metodo smo testirali na področju Ljubljane. Celoten koncept optimizacije smo najprej preizkusili na komercialnem mobilnem omrežju. Rezultati so pokazali, da

je možno s spreminjanjem različnih parametrov baznih postaj (oddajna moč, smer in lokacija antene) optimizirati ključne karakteristike omrežja (pokritje, interferenca in kapaciteta). V nadaljevanju smo v sistem dodali zračne bazne postaje in analizirali soobstoj obeh sistemov. Analizirali smo tudi možnost zagotavljanja komunikacij v izrednih razmerah le z začasnimi zračnimi in zemeljskimi baznimi postajami. Rezultati kažejo, da so zračne postaje nameščene na LAP-ih izjemno uporabne predvsem za zagotavljanje širokega pokritja omrežja v prvih fazah reševalnih operacij, z dodatnimi zemeljskimi postajami pa zagotavljamo ustrezno kapaciteto omrežja v kasnejših fazah.

Preostanek prispevka ima sledečo strukturo. Drugo poglavje vsebuje predstavitev projekta ABSOLUTE in prikaz same arhitekture omrežja za izredne razmere, ki je predlagana v projektu. V tretjem poglavju podajamo celoten postopek optimizacije vključno z orodjem za načrtovanje omrežij, evolucijskim algoritmom in kriterijskimi funkcijami. Opise vhodnih podatkov, računalniških zmogljivosti in računskih časov vsebuje poglavje štiri. V naslednjem poglavju analiziramo simulacijska scenarija postavitve in optimizacije omrežij v izrednih razmerah. Prispevek zaključimo s poglavjem šest, ki vsebuje sklepne ugotovitve.

II. PROJEKT ABSOLUTE

Osnovni cilj projekta ABSOLUTE je načrtovanje in potrditev inovativne celovite omrežne arhitekture, ki zagotavlja zanesljive komunikacijske storitve in izpolnjuje sledeče zahteve [5]:

- hitra postavitev, prilagodljivost, razširljivost in rekonfigurabilnost,
- zagotavljanje širokopasovnih storitev,
- prožnost, razpoložljivost in varnost,
- integracija tehnologije LTE-A z naprednimi satelitskimi komunikacijami in obstoječimi omrežji javne varnosti ter enot za zašito in reševanje (TETRA)

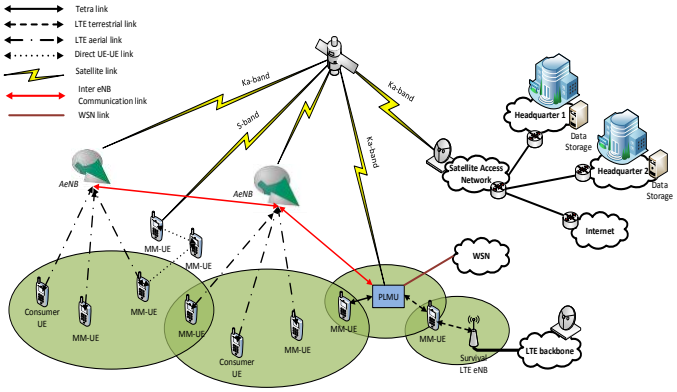
Z oportunističnim združevanjem zračnih, zemeljskih in satelitskih komunikacijskih povezav bo izboljšana razpoložljivost omrežja in omogočena hitra ter postopna vzpostavitev omrežja. Brezšivno prilagodljivo in močno razširljivo omrežno okolje vključuje tudi podporo za ustrezno stopnjo mobilnosti in energetske učinkovitosti.

A. *Arhitektura*

Arhitekturo omrežja ABSOLUTE prikazuje slika 1, kjer so prikazani različni elementi omrežja in komunikacijske povezave. Ključna ideja arhitekture omrežja je v hitri konfiguraciji in vzpostavitvi širokopasovnega omrežja, ki je omogočeno z zračnega in zemeljskega segmenta. V zračnem segmentu so uporabljene zračne bazne postaje (AeNB) nameščene na posebnih zračnih plovilih (LAP - – Low Altitute Platforms), v drugem segmentu pa mobilne zemeljske bazne postaje (PLMU - – Portable Land Mobile Unit). Obseg izrabe obeh segmentov je odvisen tako od zahtev po pokritju področja in razširljivosti operacije kot tudi gostote omrežja, ki zagotavlja namensko pasovno širino, in interoperabilnost z obstoječimi sistemi.

Glavni gradniki omrežja ABSOLUTE so:

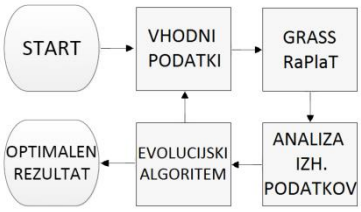
- zračna bazna postaja LTE-A (AeNB) nameščena na nizko letečo platformo (LAP), ki zagotavlja visoke prenosne hitrosti in pokritje obsežnega območja
- mobilne zemeljske postaje (PLMU) vsebujejo naslednje mobilne komunikacijske bazne postaje (LTE ali UMTS), bazno postajo TETRA, dostopovno točko WiFi in dostopno točko brezžičnega senzorskega omrežja ter hrbtenično širokopasovno satelitsko povezavo v Ka frekvenčnem pasu PLMU zagotavlja tudi interoperabilnost med različnimi komunikacijskimi sistemi.,
- napredna več-sistemska profesionalna LTE-A naprava (MM-UE – MultiMode-User Equipment), ki omogoča LTE komunikacijo v neposrednem načinu delovanja (LTE D2D) in neposredno storitev pošiljanja sporočil preko satelitske povezave v S pasu v primeru, da se nahaja zunaj pokritja AeNB-ja oziroma PLMU-ja.



Slika 1: Arhitektura omrežja ABSOLUTE

III. ORODJE ZA OPTIMIZACIJO MOBILNEGA OMREŽJA

Postopek optimizacije omrežja, prikazan na sliki 2, je razdeljen na več korakov. Jedro orodja sestavljata del za izračun pokritja omrežja in interference ter evolucijski del, ki išče nabor optimalnih rešitev.



Slika 2: Blok diagram optimizacijskega orodja

A. *GRASS-RaPlaT*

Načrtovanje omrežja je izvedeno z orodjem GRASS-RaPlaT [3], ki je bilo razvito kot dodatek orodju GRASS (Geographic Resources Analysis Support System) [6]. GRASS je odprtokodni geografski informacijski sistem, ki deluje z rastrskimi in vektorskimi podatki. Vsebuje metode za upravljanje s podatki, obdelavo slik, izdelavo map in prikaz. Jedrni moduli in knjižnice so napisani v programskem jeziku C. GRASS okolje ima zelo dobro podprte vmesnike za programiranje aplikacij (API) z več sto funkcijami, dostopnimi za programiranje novih modulov. Obdelava podatkov je avtomatizirana z uporabo skriptnih jezikov.

RaPlaT je odprtokodno modularno planersko orodje v okolju GRASS, razvito na Institutu Jožef Stefan. Uporablja se za analizo pokritosti terena z radijskim signalom in za načrtovanje omrežij. Pri izračunih upošteva različne parametre baznih postaj (oddajna moč, nagib in smer anten, itd.). V orodju so implementirani različni modeli za izračun izgube poti v ruralnem in urbanem okolju. Postopek izračuna pokritja področja z radijskim signalom sestavlja izračun izgube poti za izotropni vir, izračun pokritja za izbran tip antene in njene namestitve ter generiranje podatkov za celotno pokritje radijskega celičnega omrežja. Posamezni koraki so med seboj povezani s skripto *r.radcov* napisano v programskem jeziku Python.

B. *Evolucijski algoritem*

Evolucijski algoritmi (EA) so stohastični optimizacijski algoritmi, ki delujejo na principih privzetih iz biološke evolucije [7]. Poiščejo optimalne argumente, ki jim rečemo tudi rešitve, za podano kriterijsko funkcijo tako, da začnejo iz naključne populacije rešitev, ki jih nato v iteracijah mutirajo in medsebojno križajo v vse boljše rešitve. Ker za vsako smiselno optimizacijo velja, da njene rešitve konvergirajo, se algoritem ustavi takrat, ko se z dodatnimi iteracijami populacija rešitev ne izboljšuje več. Več-kriterijska optimizacija išče optimalne rešitve po več kriterijih hkrati ter jih primerja po Pareto optimalnosti. Rezultat več-kriterijskega EA-ja je množica Pareto optimalnih rešitev, to je rešitev, ki predstavljajo različne kompromise med optimalnostjo posameznih kriterijev in za katere velja, da nobena ni slabša od ostalih v vseh kriterijih. Konvergenca več-kriterijskega EA-ja se ugotavlja tako, da se v vsaki iteraciji izračuna hipervolumen, ki ga omejuje na eni strani Pareto fronta optimalnih rešitev ter na drugi strani referenčna točka, ki je nastavljena tako, da je slabša od vseh možnih rešitev. EA-ji omogočajo relativno enostavno paralelizacijo in AMS-DEMO je primer učinkovite vzporedne implementacije.

C. *Optimizacijski postopek*

Komunikacija med evolucijskim algoritmom AMS-DEMO in orodjem GRASS-RaPlat upravlja Python skripta. Njeno psevdo kodo podaja algoritem 1.

EA iterativno izvaja prilagajanje vhodnih podatkov in oceni obdelane rezultate imenovane rešitve. Omrežni parametri, ki so ocenjeni v predhodni iteraciji, so posredovani v GRASS-RaPlaT in obdelani z modulom *r.radcov*. Modul *r.radcov* izvede izračun izgube poti z izboljšanim modelom Okumura-Hata [3], ki z upoštevanjem profila terena, podatkov o rabi tal in senčenju, zagotavlja realistične rezultate za mestna, primestna in podeželska področja. Za izračun najmočnejšega signala in nivoja vseh ostalih motilnih signalov za vsako točko rastra upošteva še oddajno moč in sevalni diagram antene. V nadaljevanju so obdelani vhodni podatki analizirani glede na izbrane kriterijske funkcije in poslani v EA, kjer se izvaja vrednotenje. Na podlagi najboljših predhodnih rezultatov, EA izračuna nove vhodne podatke in prične novo iteracijo. Cilj opisanega iterativnega optimizacijskega postopka je maksimiranje vseh kriterijskih funkcij.

D. *Kriterijske funkcije*

Za optimizacijo mobilnega omrežja smo izbrali tri kriterijske funkcije: (i) pokritje, (ii) SINR in (iii) kvaliteta. Dodatno smo določili še pogojno funkcijo imenovano (iv) zasedenost, kateri morajo zadostiti vsi elementi iz množice rešitev.

Algorithm 1 Python script

```
initialization
connecting to GRASS environment
starting r.radcov module
csv1 ← coverage processed data output
csv2 ← SINR processed data output
csv3 ← quality processed data output
csv4 ← maximum occupancy (N_max) per cell output
N_ref ← allowed cell occupancy output
i, m ← No. of raster points below the threshold
j, n, y ← No. of all raster points
loop
    if N_max < N_ref then
        for all (csv1) do
            if csv1 > -95 dBm then
                i ← i + 1
            j ← j + 1
        for all (csv2) do
            if csv2 > 6 dB then
                m ← m + 1
            n ← n + 1
        for all (csv3) do
            x ← x + csv3
            y ← y + 1
[coverage, SINR, quality ← [i/j, m/n, x/y]
output calculated data into .txt file
```

- **Pokritost** je delež točk na zemljevidu, pri katerih je sprejeta moč signala višja od zahtevane mejne vrednosti -95 dBm. Izbrana vrednost predstavlja mejni nivo sprejetega signala, ki še omogoča povezave brez izpadov.
- **SINR** je delež točk, pri katerih je razmerje moči koristnega sprejetega signala in skupne interference večji od 6 dB pri predvideni polni obremenitvi sistema. Uporablja se za identifikacijo kritičnih robnih delov celic, kjer so zaradi manjšega pretoka uporabnikom na voljo okrnjene storitve. S povečevanjem vrednosti SINR je za preprečevanje interference potrebno manj koordinacije znotraj celice in med celicami, posledično pa se poveča tudi kapaciteta sistema.
- Kriterijska funkcija **kvaliteta** je povprečje vrednosti kvalitet v vseh točkah izbranega območja. Pri tem se za posamezno točko kvaliteto določi kot razmerje teoretične spektralne učinkovitosti, izračunane s pomočjo SISO (Single Input - Single Output) Shannon-ove formule za kapaciteto, in fiktivne vrednosti števila uporabnikov, ki je za posamezno točko na zemljevidu določeno glede na tip terena. Za referenco se uporablja kvaliteta izračunana za originalno postavitev omrežja in nastavitev anten.
- **Zasedenost** predstavlja skupno število uporabnikov znotraj posameznega sektorja. Uporabljamo jo z namenom, da pri optimizaciji ne bi prekoračili normalnih obremenitev v smislu prenosnih kapacitet, ki jih lahko najdemo pri radijskih celicah v realnih omrežjih. Zasedenost je izračunana s seštevanjem uporabnikov, pri čemer se upošteva točke, kjer najmočnejši sprejeti signal pripada isti celici. Referenčna vrednost je dobljena z izračunom zasedenosti najbolj zasedene celice pri originalni postavitvi anten. Ta vrednost je določena kot maksimalna dopustna vrednost zasedenosti katerekoli celice pri optimizaciji.

IV. VHODNI PODATKI

Orodje za optimizacijo zahteva več različnih vhodnih podatkov. Ključni modul za radijsko planiranje, *r.radcov*,

prebere začetno konfiguracijsko datoteko omrežja in zemljevide okolja v rastrski obliki. Rastrski zemljevid je podatkovna plast, ki je sestavljena iz mrežastega polja celic. Vsebuje končno število stolpcev in vrstic s podatkovno točko v vsaki celici. Meje zemljevida so vpisane v poljih vzhod, zahod, sever in jug. Poleg konfiguracijske datoteke omrežja v CSV (Comma-Separated Values) obliki, sta v orodje uvožena tudi dva rastrska zemljevida; digitalni model višin (DEM – Digital Elevation Model) in zemljevid s podatki o rabi tal (Clutter data map) z ločljivostjo 25 m x 25 m.

DEM je rastrski zemljevid, ki vsebuje koordinate terena v Gauss-Krüger koordinatnem sistemu in podatke o višini posamezne rastrske točke. Zemljevid rabe tal pa vsebuje vrednosti izgube poti signala za vsako točko rastra, ki je odvisna od tipa in rabe terena. Tipične vrednosti slabljenja so bile pridobljene z meritvami in so dodeljene glede na tip terena na izbranem področju. Konfiguracijska datoteka določenega omrežja vsebuje lokacije, oddajne moči, mehanične vertikalne nagibe in višine anten ter njihove sevalne diagrame. Poleg opisanih vhodnih datotek je za izračun interference v eni rastrski točki v orodju za optimizacijo možno določiti še oddajno frekvenco, model izgube poti, število procesorjev za večprocesno obdelavo in število upoštevanih signalov iz različnih oddajnikov. Za optimizacijo lokacij baznih postaj so dodatno upoštevane tudi lokacije stavb, ki so v simulacijsko okolje uvožene kot rastrski zemljevid.

Prikazani scenariji temeljijo na obstoječi konfiguraciji komercialnega radijskega omrežja na področju Ljubljane velikosti 122.6 km^2 z originalnimi nastavitvami smeri in nagibov anten. Na vsaki bazni postaji je bila oddajna moč posamezne antene nastavljena na 46 dBm, mehanski vertikalni nagib anten se je spreminjal od -20º do 10º, smer anten pa je bila nastavljena na tipične vrednosti 30º, 150º oziroma 270º.

Za učinkovito izkoriščanje možnosti paralelizacije evolucijskih algoritmov, deluje AMS-DEMO na gruči tridesetih računalnikov. Vsak od njih ima vgrajen Intel Xeon 5220 procesor in 6 GB delovnega pomnilnika. Na vsakem računalniku se hkrati izvaja le ena simulacija. Celotni simulacijski čas razdelimo na procesni čas za radijsko planiranje, čas za ocenjevanje rešitev in čas za iskanje optimalnih rešitev z AMS-DEMO. Procesni čas je odvisen od števila anten, velikosti analiziranega območja, ločljivosti rastrskih podatkov in izbranega modela izgube poti. Celotni čas optimizacije je močno odvisen tudi od razpoložljive računalniške moči in števila iteracij, ki so potrebne, da optimizirano omrežje doseže želene zmogljivosti.

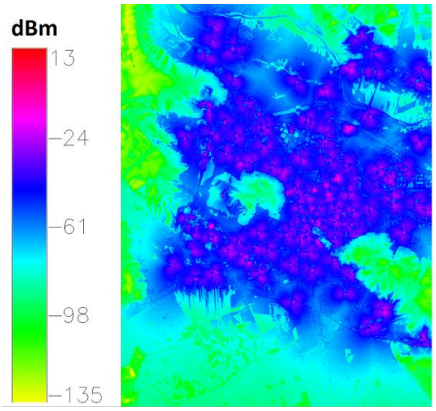
V. REZULTATI POSTAVITVE IN OPTIMIZACIJE OMREŽJA V IZREDNIH RAZMERAH

V nadaljevanju bomo predstavili dva simulacijska scenarija, ki opisujeta postavitev in optimizacijo omrežja za izredne razmere. V prvem scenariju predvidevamo popolno okvaro obstoječega omrežja in izgradnjo začasnega omrežja, ki ga v nadaljevanju dograjujemo s postopnim vključevanjem komercialnih baznih postaj. V drugem scenariju predvidevamo, da obstoječih omrežij ni možno obnoviti in je treba vzpostaviti popolnoma samozadostno komunikacijsko omrežje. V obeh scenarijih smo upoštevali zahteve po maksimalni pokritosti prizadetega področja, minimalni interferenci med posameznimi celicami in čim višji kapaciteti povezav.

A. *Postopna izgradnja omrežja*

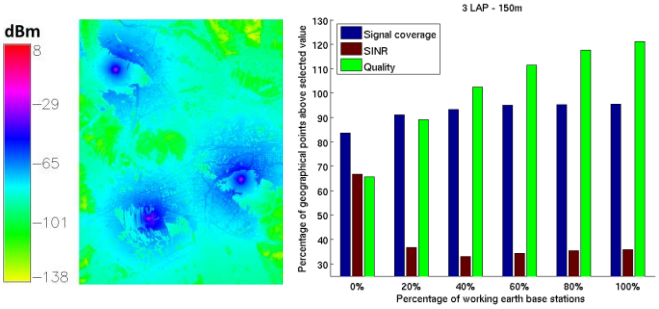
V tem scenariju predvidevamo hudo nesrečo, ki povzroči popolno okvaro obstoječega mobilnega omrežja. Komunikacije so postopoma ponovno vzpostavljene; najprej z nekaj nizko-letečimi platformami (LAP), ki imajo nameščene bazne postaje (AeNB), in so razporejene nad prizadetim področjem. V naslednjem koraku pa sledi ponovno vključevanje obstoječih komercialnih baznih postaj. V testnem primeru so bazne postaje vključene v omrežje v petih korakih. V vsakem koraku je vključenih 20% naključno izbranih baznih postaj. Preizkusili smo primere s tremi oziroma šestimi LAP-i, ki so bili nameščeni na isti višini. Obe testni konfiguraciji smo preizkusili na treh različnih višinah: 150 m, 200 m in 300 m. Skupna analiza je zajemala šest pod-scenarijev, ki so analizirani v nadaljevanju. Oddajno moč zračne bazne postaje AeNB smo nastavili na 48 dBm, medtem ko so bile oddajne moči zemeljskih baznih postaj nastavljene na 46 dBm.

Pokritje originalnega omrežja komercialnega mobilnega operaterja na področju Ljubljane prikazuje slika 3. V tem primeru je vrednost kriterijskih funkcij »pokritje« in »SINR« 92.4% oziroma 25%.

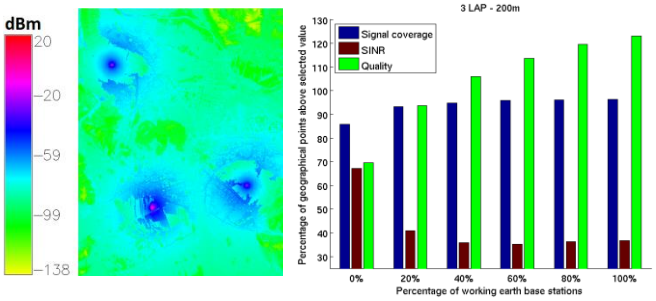


Slika 3: Originalna namestitev baznih postaj mobilnega operaterja v Ljubljani

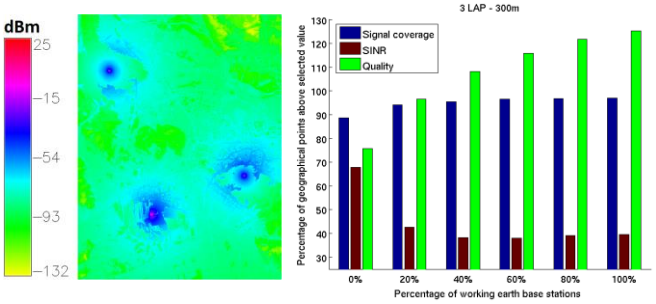
V nadaljevanju so podani rezultati za opisane konfiguracije postopnega vzpostavljanja komunikacijskega omrežja v izrednih razmerah. Slike 4, 5, in 6 predstavljajo rezultate s tremi vzpostavljenimi LAP-i. Slike 7, 8 in 9 pa rezultate s šestimi vzpostavljenimi LAP-i. Položaji LAP-ov so optimizirani s predhodno opisanim optimizacijskim orodjem.



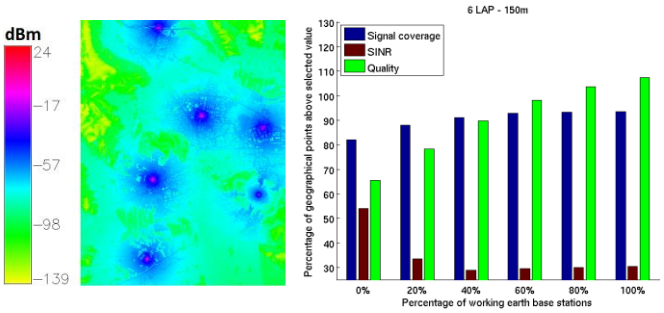
Slika 4: 3 LAP-i na 150 m



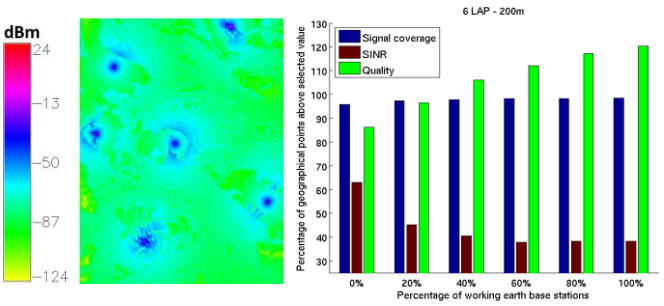
Slika 5: 3 LAP-i na 200 m



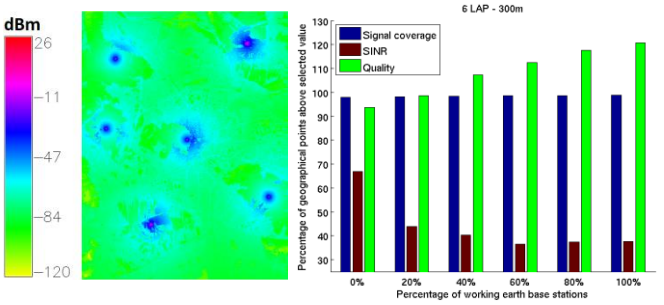
Slika 6: 3 LAP-i na 300 m



Slika 7: 6 LAP-ov na 150 m



Slika 8: 6 LAP-ov na 200 m



Slika 9: 6 LAP-ov na 300 m

Pri analizi smo upoštevali vse kriterijske funkcije. Medtem ko sta »pokritje« in »SINR« v absolutnem razmerju z največjo možno vrednostjo 100%, »kvaliteta« vsebuje relativno informacijo o kvaliteti omrežja v smislu dosegljivih prenosnih bitnih hitrostih glede na izbrano referenčno omrežje. Zato lahko vrednost kvalitete preseže 100%. V analizi smo za referenco izbrali originalno omrežje mobilnega operaterja brez dodatnih LAP-ov.

Simulacijski rezultati kažejo, da je možno z AeNB-ji relativno hitro pokriti razmeroma veliko področje in na ta način začasno učinkovito nadomestiti komercialno omrežje. Procent pokritja področja z radijskim signalom je odvisen od števila nameščenih LAP-ov in njihove višine nad tlemi. Z uporabo treh LAP-ov je z radijskim signalom možno pokriti med 80% in 90% področja, s šestimi LAP-i pa je možno doseči več kot 90% pokritje. Poleg tega je odstotek točk, ki imajo zadovoljivo razmerje SINR veliko višje v primeru, ko so nameščeni le LAP-i (približno 60%). S postopnim ponovnim vzpostavljanjem zemeljskih postaj se SINR poslabšuje in pade na vrednosti okoli 30%. To kaže, da je vključevanje zemeljskega omrežja nepotrebno oziroma celo nezaželeno, saj bistveno ne izboljša geografskega pokritosti in povečuje interferenco. Pridobljene koristi se skrivajo v zadnjem kriteriju, »kvaliteti«, ki predstavlja merilo kapacitete pasovne širine, ki jo zagotavlja omrežje. Omrežje LAP-ov zagotavlja bistveno manjšo kapaciteto v primerjavi z originalnim omrežjem mobilnega operaterja. S postopnim vključevanjem zemeljskih postaj je povečanje »kvalitete« in posledično kapacitete omrežje razvidno v vseh šestih primerih. Ko so vse zemeljske postaje ponovno vključene v omrežje, »kvaliteta« celotnega omrežja skupaj z AeNB doseže vrednost 120%.

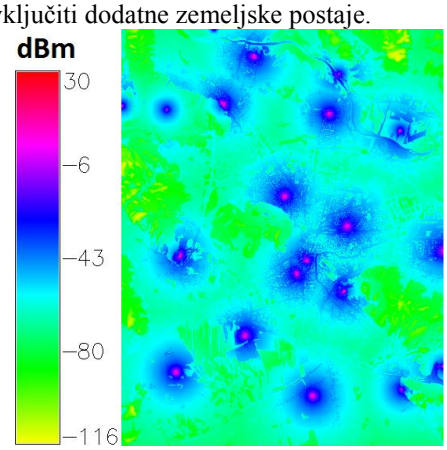
Število LAP-ov in njihova višina pomembno vpliva na vse tri kriterijske funkcije, zlasti v prvi fazi vzpostavitve omrežja. Z večanjem števila LAP-ov in njihove višine se zmogljivost omrežja izboljšuje. To potrjujejo tudi simulacije, saj omrežje s šestimi LAP-i na višini 300 m zagotavlja najboljše zmogljivosti omrežja.

B. *Vzpostavitev samozadostnega omrežja za izredne razmere*

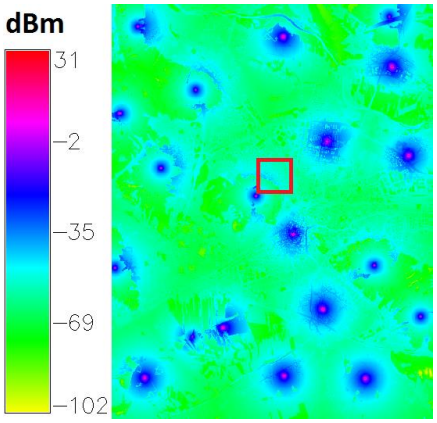
V tem scenariju predvidevamo, da zmogljivosti obstoječih omrežij operaterjev ni možno obnoviti in je treba vzpostaviti samozadostno komunikacijsko omrežje za izredne razmere. V testnem scenariju število uporabljenih zračnih (AeNB) in zemeljskih baznih (PLMU) postaj ni omejeno. V optimizaciji je, poleg predhodno izbranih kriterijskih funkcij, vključena dodatna funkcija, ki določa minimalno število vseh uporabljenih postaj. V simulaciji obravnavamo isto področje Ljubljane kot v predhodnem scenariju, ki smo mu dodali manjše popolnoma nedostopno področje. V tem področju kvadratne oblike ni možno postaviti nobene bazne postaje, vendar je kljub temu treba reševalnim ekipam na tem področju zagotoviti komunikacijo. Analizirali smo tri različne velikosti, in sicer 1x1 km^2, 2x2 km^2 in 3x3 km^2. Dobljeni rezultati so bili optimizirani za dosego najboljšega možnega pokritja in vrednosti SINR. V povprečju je bilo z radijskim signalom pokritih okoli 98% točk, zadovoljivo visok SINR pa je bil zagotovljen v nekaj manj kot 60% točk.

Rezultate prikazujejo slike 10, 11, 12 in 13. Število baznih postaj narašča z velikostjo nedostopnega področja, kar je pričakovani rezultat. Manj pričakovano je razmerje med številom uporabljenih AeNB-jev in PLMU-jev. Razvidno je, da so AeNB-ji veliko bolj zaželena izbira, saj zagotavljajo večje pokritje. Celotno območje Ljubljane je mogoče pokriti z 20 LAP-i in dvema PLMU-jema. Kapaciteta takega sistema zadostuje komunikacijskim potrebam osebja za posredovanje v izrednih razmerah (first responders). Za nadaljnje

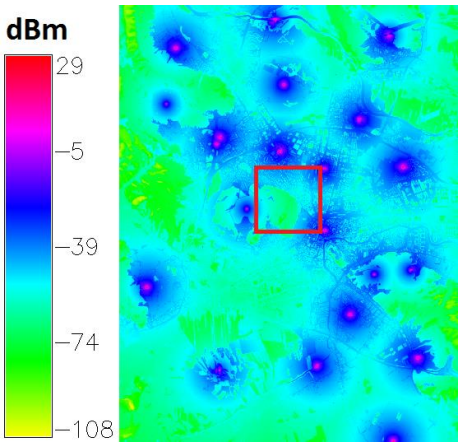
izboljšanje »kvalitete« pa bi bilo treba, podobno kot v prvem scenariju, vključiti dodatne zemeljske postaje.



Slika 10: Brez nedostopnih področij – 19 LAP-ov, 1 PLMU, 97.9% pokritje, SINR 58.3%



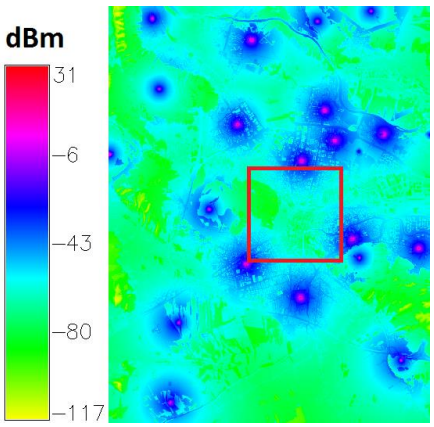
Slika 11: Nedostopno področje velikosti 1 kmx1 km - 20 LAP-ov, 0 PLMU-jev, 99.9% pokritje, SINR 58.5%



Slika 12: Nedostopno področje velikosti 2 kmx2 km - 19 LAP-ov, 2 PLMU-ja, 98.5% pokritje, SINR 57.6%

VI. ZAKLJUČEK

V prispevku smo predstavili orodje za optimizacijo brezžičnih omrežij, ki temelji na orodju za radijsko planiranje GRASS-RaPlaT in evolucijskem algoritmu AMS-DEMO. Bistvena prednost orodja je v uporabi realnih geografskih podatkov o okolju, kar povečuje praktično vrednost rezultatov.



Slika 13: Nedostopno področje velikosti 3 kmx3 km - 19 LAP-ov, 3 PLMU-ji, 98.8% pokritje, SINR 55.4%

Eksperimente smo izvedli na področju Ljubljane, velikosti 122,6 km^2. V analizah smo upoštevali tudi podatke o omrežju mobilnega operaterja, ki ima na tem področju postavljenih 325 baznih postaj na frekvenci 900 MHz.

Analizirali smo dva različna scenarija: (i) soobstoj arhitekture za komunikacije v izrednih razmerah z obstoječim komercialnim mobilnim omrežjem in (ii) upravljanje topologije baznih postaj, ki je sestavljena iz zračnih (AeNB) in zemeljskih (PLMU) baznih postaj.

Rezultati so potrdili, da so AeNB-ji izjemno učinkoviti za hitro zagotovitev radijskega pokritja razmeroma velikih področij (6 LAP-ov je dovolj za celo področje Ljubljane). S primerno medsebojno oddaljenostjo AeNB-jev je možno zagotoviti tudi dovolj nizko interferenco. Bistvena pomanjkljivost, ki jo kažejo simulacijski rezultati, je v omejeni kapaciteti omrežja, ki jo je možno povečati le z vključitvijo znatnega števila manjših zemeljskih celic (bazne postaje obstoječih komercialnih omrežij ali dodatni PLMU-ji). Torej so AeNB-ji primerni predvsem za zagotavljanje komunikacij omejenemu številu uporabnikom v izrednih razmerah. Za zagotavljanje komunikacijskih zmogljivosti v primeru začasnih dogodkov z veliko gostoto uporabnikov pa sami AeNB-ji niso dovolj.

ZAHVALE

Prispevek temelji na raziskovalnem delu, ki ga delno sofinancira evropska komisija preko projekta sedmega okvirnega programa ABSOLUTE (FP7-ICT-2011-8-318632).

LITERATURA

[1] N. Weicker, G. Szabo, K. Weicker, and P. Widmayer, "Evolutionary multiobjective optimization for base station transmitter placement with frequency assignment," IEEE Transactions on Evolutionary Computation, vol. 7, pp. 189-203, 2003.

[2] G. E. Athanasiadou, D. Zarbouti, and G. V. Tsoulos, "Automatic location of base-stations for optimum coverage and capacity planning of LTE systems," in Proc. 8th European Conf. Ant. and Prop. (EuCAP), 2014, pp. 2077- 2081.

[3] I. Ozimek et al., "GRASS-RaPlaT - an open-source tool for radio coverage calculations, " IEEE Joint Workshop on Wireless Commun., France section, Paris, March 2011.

[4] M. Depolli, R. Trobec, and B. Filipič, "Asynchronous master-slave parallelization of differential evolution for multiobjective optimization," Evolutionary Computation, pp. 261-291, May 2013.

[5] Projekt ABSOLUTE internetna stran: http://www.absolute-project.eu/.

[6] GRASS GIS internetna stran, http://grass.osgeo.org.

[7] G. Jones: Genetic and Evolutionary Algorithms, Encyclopedia of Computational Chemistry, John Wiley & Sons, Ltd., 2002.

Andrej Vilhar je na Odseku za komunikacijske sisteme Instituta "Jožef Stefan" zaposlen od leta 2004, opravlja pa tudi delo asistenta na Mednarodni podiplomski šoli Jožefa Stefana. Diplomiral in doktoriral je na Fakulteti za elektrotehniko v Ljubljani leta 2004 oziroma 2009. Tema njegove doktorske disertacije je bila optimizacija postopkov za hierarhično upravljanje mobilnosti v internetu. Po doktoratu se je usmeril na področje razširjanja radijskih valov. Eno leto je kot podoktorski sodelavec delal na francoski raziskovalni instituciji ONERA. Sodeluje na različnih mednarodnih in domačih raziskovalnih in aplikativnih projektih povezanih s profesionalnimi mobilnimi komunikacijskimi sistemi, in s razširjanjem visokofrekvenčnih satelitskih signalov.

Andrej Hrovat je na Odseku za komunikacijske sisteme Instituta "Jožef Stefan" zaposlen od leta 2004, v zadnjem obdobju na mestu znanstvenega sodelavca. Poleg tega je tudi asistent na Mednarodni podiplomski šoli Jožefa Stefana. Diplomiral in magistriral je na Fakulteti za elektrotehniko v Ljubljani leta 2004 oziroma 2008. Leta 2011 je doktoriral na Mednarodni podiplomski šoli Jožefa Stefana. Sodeluje na različnih mednarodnih in domačih raziskovalnih in aplikativnih projektih povezanih s profesionalnimi mobilnimi komunikacijskimi sistemi, 2/3G, WiFi in WiMAX tehnologijami, satelitskimi in senzorskimi omrežji.

Tomaž Javornik ja zaposlena kot znanstveni svetnik na Odseku za komunikacijske sisteme Instituta "Jožef Stefan". Opravlja pa tudi delo docenta na Mednarodni podiplomski šoli Jožefa Stefana. Diplomiral, magistriral in doktoriral je na Fakulteti za elektrotehniko v Ljubljani leta 1987, 1990 oziroma 1993. Kot gostujoči znanstvenik je šest mesecev deloval na univerzi Westminster v Londonu, Velika Britanija. Raziskovalno se ukvarja predvsem z razširjanjem radijskih signalov, modeliranjem kanalov v zemeljskih in satelitskih komunikacijskih sistemih, adaptivnim kodiranjem in modulacijami, prilagodljivimi antenskimi MIMO sistemi, brezžično optiko.

Mobilna omrežja v izrednih razmerah

Iztok Saje, Telekom Slovenije

Povzetek: Mobilna omrežja imajo vse bolj pomembno vlogo ob izrednih razmerah. Veliko število baznih postaj in podvojeni elementi jedrnega omrežja zagotavljajo visoko razpoložljivost. Prihajajoče zlivanje zasebnih in javnih omrežij postavlja nove zahteve po funkcijah sistema ter zanesljivosti delovanja. Mobilna omrežja je potrebno upoštevati v državnih strategijah in pripravah za reševanje v izrednih razmerah.

Ključne besede: VITEL, izredne razmere, 700 MHz, mobilna omrežja

Abstract: The role of public mobile networks in emergency situation is increasing. Private and public mobile radio networks convergence puts new demands on 3GPP standardization and network architecture.

Keywords: VITEL, emergency communications, 700 MHz, mobile networks

I. UVOD

Na delavnici VITEL o varnosti v telekomunikacijskih omrežjih pred 12 leti je bil objavljen članek z istim naslovom, ki še danes ni zastarel.

Tehnologijo GSM nadomeščata tehnologiji UMTS in LTE. Poleg govora se na mobilna omrežja seli tudi velik del prometa in s tem je delovanje mobilnih omrežjih ob izrednih dogodkih še bolj nujno. Poleg omogočanja osebnih povezav, zagotavljajo tudi delovanje sistemov, ki temeljijo na povezavi naprav (internet stvari).

TETRA in podobni zasebni sistemi so namenjeni predvsem za govor in ne omogočajo visokopretočnih storitev. Na področju standardizacije in regulacije poteka veliko sprememb, pričakujemo lahko, da bo prišlo do zlivanja javnih in zasebnih radijskih omrežij in s tem se bodo povečale zahteve po razpoložljivosti javnih mobilnih omrežij.

II. ARHITEKTURA OMREŽIJ

Osnovni gradnik mobilnih omrežij, ki zagotavlja radijsko pokrivanje, so bazne postaje. Te so s prenosnimi sistemi povezane z jedrnim omrežjem. Dostopovno omrežje zajema bazne postaje, prenosne sisteme in krmilnike baznih postaj (BSC, RNC) ter zagotavlja povezavo med jedrnim omrežjem in terminalom.

Tehnologije GSM, UMTS in LTE standardizira organizacija 3GPP in so med seboj usklajene, tako da terminali samodejno prehajajo med tehnologijami.

Pri kompleksnih omrežjih je prilagoditev na nepričakovane izpade zelo zahtevna in je ne moremo prepustiti samo mehanizmom za samodejno zagotavljanje delovanja. V izrednih razmerah je kritičnega pomena usposobljena in strokovna ekipa, ki pozna tehnologijo in arhitekturo omrežja.

A. Jedrno omrežje

S klasične arhitekture GSM (MSC, SGSN, GGSN, HLR) smo prišli na veliko bolj zahtevno arhitekturo v okviru EPC (Evolved Packet Core), kjer se tudi klasične govorne storitve selijo med paketne storitve (govor prek LTE, VoLTE).

Nova arhitektura povečuje zanesljivost sistema, saj so dostopovni sistemi povezani na več strežnikov in s tem je zmanjšana možnost večjih izpadov. Omrežni elementi v jedrnem omrežju so postavljeni na več lokacijah.

B. Prenosni sistemi v radijskem dostopu

V zadnjih letih poteka intenzivna nadgradnja prenosnih sistemov iz PDH (GSM) in ATM (UMTS) na Ethernet/IP, sočasno z izgradnjo LTE omrežij. Visoke zahteve po prepustnosti baznih postaj (trenutno do 300 Mb/s, kmalu preko 1 Gb/s) ter arhitektura porazdeljenih baznih postaj (t.i. "izdovojeni baseband") zahtevajo optične povezave, ki vse bolj nadomeščajo mikrovalovne povezave in ostale tehnologije.

Zanesljivost prenosnih sistemov zagotavlja IP/MPLS ter podvojene povezave med vozlišči. Do samih baznih postaj poteka samo ena povezava, na podeželju je pogosta zaporedna vezava dveh in več baznih postaj. Lokacije, kjer se združuje prenos za več baznih postaj, imajo večinoma podvojeno povezavo proti jedrnem omrežju ter dodatno baterijsko napajanje.

C. Bazne postaje

Na lokaciji bazne postaje so antene in radijska oprema, ki zagotavljajo radijsko pokrivanje z omrežji GSM, UMTS in LTE na različnih frekvenčnih pasovih.

Usmerjene antene razdelijo pokrivanje v več sektorjev (najpogosteje tri). Sodobna tehnologija omogoča, da ista radijska glava s sprejemniki in oddajniki deluje na dveh tehnologijah in dveh frekvenčnih pasovih, pogosto GSM in LTE na pasovih 900 in 1800 MHz, GSM in UMTS na pasu 900 MHz ter kmalu UMTS in LTE na frekvenčnem pasu 2100 MHz.

Radijske glave so pogosto postavljene ob antenah, saj se s tem izognemo slabljenju v koaksialnih kablih. Izpad ene radijske glave samo zmanjša pokrivanje v eni celici, saj večino prometa prevzamejo druge celice in tehnologije. Prekrivanje s sosednjimi baznimi postajami omogoča brezprekinitveni prehod med celicami (handover), tako da ob izpadu cele bazne postaje del prometa prevzamejo sosednje.

Najpogostejše nedelovanje je posledica modernizacije in nadgradenj omrežja, saj se ob posegih na antenah ugasnejo vsi oddajniki vseh operaterjev na lokaciji. Kot vzrok izpada sta pogosta tudi izpad prenosnih sistemov in napajanja, medtem ko so okvare na antenah in radijski opremi redke. Veliko bolj redko izpade cela lokacija, vendar se je že zgodilo, da je zgradba pogorela ali se enostavno podrla.

Vse bazne postaje imajo baterijsko napajanje, ki zagotavlja več ur delovanja brez zunanjega napajanja. Zaradi visoke cene napajanje z vetrom in sončnimi celicami ni pogosto. Ob daljših izpadih zunanjega napajanja je edina rešitev napajanje z zunanjim generatorjem, ki ga začasno pripeljemo na lokacijo. Nove napajalne tehnologije, kot so

gorivne celice, bodo lahko zagotavljale daljše obratovanje ob izpadih energetskega omrežja.

III. ŽLED

Februarja 2014 je žled prizadel velik del Slovenije. Zaradi izpada napajanje je bilo okrnjeno delovanje vseh sistemov in marsikje so bile možne povezave samo prek satelitskih sistemov (predvsem Thuraya) in prek radioamaterskih postaj.

V mobilnem omrežju Telekoma Slovenije je istočasno izpadlo 200 baznih postaj, velika večina zaradi izpada napajanja. Optično omrežje je bilo manj prizadeto.

Prvi ukrep je bil dvig prepustnosti na delujočih baznih postajah, ki so pokrivale prizadeto območje in kjer je to bilo možno. Proizvajalec opreme Ericsson je dovolil, da smo izklopili vse licenčne omejitve, kot so število sočasnih zvez, moči oddajnikov in podobno.

Terenske ekipe so intenzivno odpravljale napake ter opremile vrsto lokacij z agregati. Pripomoglo je tudi usklajevanje z drugimi operaterji, gasilci, civilno zaščito itd.

Poleg ukrepov na omrežju smo operaterji na prizadetem območju pomagali s SIM karticami, kjer je pokrivalo samo eno omrežje. V ponudbi imamo tudi najem satelitskih terminalov, ki so tudi nadomestili običajne povezave.

IV. ZLIVANJE JAVNIH IN ZASEBNIH SISTEMOV

Zasebni radijski sistemi (predvsem TETRA, vendar tudi ostali) so primerljivi s sistemom GSM in ne omogočajo visokopretočnih internetnih storitev.

Storitve v oblaku, dostop do baz podatkov, dokumentacije in podobno zahtevajo ustrezno rešitev. V nekaterih državah (ZDA) se pripravljajo na gradnjo državnega omrežja LTE samo za izbrane uporabnike, v Evropi bo prevladalo zlivanje med omrežji, kjer bo omrežje TETRA navidezni operater na javnih omrežjih LTE.

A. 700 MHz in TETRA

Evropa se pripravlja na podelitev frekvenčnega pasu 700 MHz za javna omrežja. Poleg dvakrat po 30 MHz za javna omrežja LTE (iste frekvence kot v Aziji in na Pacifiku) so na razpolago še frekvence, za katere v EU uporaba še ni dogovorjena.

V Sloveniji se ta podelitev povezuje z modernizacijo omrežja TETRA, kljub temu, da tehnično ni nobene povezave. Uporabniki sistema TETRA v javnem omrežju LTE bodo uporabljali vse frekvenčne pasove v tem omrežju (700, 800, 900, 1800, 2100 in 2600 MHz) in ne samo 700 MHz. Uporabniki javnih omrežij ne bodo imeli dostopa do zasebnega omrežja na frekvenčnem pasu 700 MHz.

Za operaterje je podelitev frekvenc na pasu 800 MHz pomenila veliko novost in na tem pasu gradimo osnovno pokrivanje z LTE na podeželju. Pas 700 MHz bomo uporabili samo za dvig prepustnosti z združevanjem s pasom 800 MHz ter za izboljšano pokrivanje, kjer se celice na 800 MHz pretirano prekrivajo. Prav zaradi tega ni smiselno postavljati velikih zahtev za pokrivanje samo na 700 MHz, saj je za uporabnike pomembna samo dostopnost storitev na katerem koli izmed frekvenčnih pasov.

B. Standardizacija 3GPP

V okviru organizacije 3GPP poteka standardizacija novih funkcij, ki so predvsem namenjene kritičnim komunikacijam. Tako bo možna povezava med terminali brez sodelovanja omrežja, dodatne možnosti prioritet, zaznavanje terminalov v bližini in podobno.

V. PRIPRAVLJENOST OMREŽIJ NA IZREDNE RAZMERE

Zaradi velikega števila baznih postaj, dvojnega pokrivanja in dosedanjih ukrepov je razpoložljivost javnih mobilnih omrežij zelo velika.

Trenutna državna strategija predvideva, da bodo visokopretočne storitve tekle izključno na optičnih omrežjih in ne načrtuje opazne državne pomoči pri zagotavljanju pokrivanja s tehnologijo LTE tam, kjer operaterji nimamo komercialnega interesa.

Pogosto bi lahko z minimalnimi vlaganji dosegli boljši učinek.

Kot primer: danes ima vsakdo pri sebi mobilni terminal. Ob potresu je zahtevno iskanje pogrešanih oseb in tu bi si lahko pomagali z namenskimi baznimi postajami za prestrezanje pogovorov (lovilci IMSI), ki so bili kupljeni za povsem drug namen.

Zaradi nepoznavanja delovanja omrežij prihajajo nesmiselni predlogi, kot je recimo stalno spremljanje lokacije vsakega terminala za izdelavo statistik in podobno, kar bi pomenilo nerazumno obremenitev sistema s signalizacijo, moteno delovanje storitev ter kršenje zasebnosti uporabnikov.

A. Odprte bazne postaje

Odprte bazne postaje so lepa možnost za redko poseljeno podeželje. Lokalna skupnost z državno pomočjo zgradi primeren objekt z antenskim stolpom, napajanjem ter optično povezavo, ki ga lahko uporabljajo vsi operaterji (poleg operaterjev omrežij GSM/LTE tudi operaterji omrežij DAB, DVB-T, WiFI in ostali). Poleg osnovnega pokrivanja bi zagotovili tudi dodatno pokrivanje ter s tem dvignili zanesljivost omrežij.

B. Začasne bazne postaje

Operaterji imamo mobilne bazne postaje, ki jih uporabljamo za zagotavljanje prepustnosti na prireditvah (na primer, skoki v Planici). Ob manjših izrednih dogodkih lahko z njimi rešujemo pokrivanje. Zakonodaja danes ne predvideva ustrezne prednosti za postavitev začasnih baznih postaj za zagotavljanje delovanja mobilnih storitev v primeru izrednih dogodkov.

C. Spodbujanje redundantnih mikrovalovnih povezav

Z gradnjo optičnih povezav do baznih postaj se zmanjšuje delež mikrovalovnih povezav. Zaradi varčevanja se mikrovalovne povezave izključujejo in se ne uporabljajo. Predlog AKOSa o podelitvi mikrovalovnih radiofrekvenčnih pasov pomeni, da se za posamezno zvezo ne plačuje pristojbina za uporabo radijskih frekvenc in s tem je lažje upravičiti vzporedne mikrovalovne zveze, ki zagotavljajo delovanje ob izpadu optičnih povezav.

D. Zakonodaja

Zakonodajalec pogosto ne razmišlja o stranskih učinkih ukrepov. Lep primer je nevtralnost interneta, ki ne omogoča prednostnih povezav s strežniki, namenjenimi podpori reševalnih aktivnosti ob izrednih dogodkih. Pri iskanju pogrešanih oseb je vprašljivo kršenje njihove zasebnosti.

VI. ZAKLJUČEK

Nedvomno je, da imajo mobilna omrežja veliko vlogo v izrednih razmerah, in veliko primerov je, kjer se je to pokazalo. Mobilni terminal ima vsakdo in zagotavlja osnovno komunikacijo med ljudmi in tudi med napravami.

Z zlivanjem javnih in zasebnih sistemov in prihajajočimi funkcijami omrežij 3GPP postaja še pomembnejše, da se tehnologiji GSM in LTE upoštevata pri načrtovanju ukrepov v primeru izrednih razmer ter ustrezni regulaciji.

Manjka celovita razprava o vlogi mobilnih omrežij. Pogosto se ukvarjamo samo z enim izmed izzivov (delovanje 112, problematika 700 MHz, ipd). V okviru priprave strategij bi morali bolj upoštevati, kaj omogočajo današnje in prihajajoče tehnologije in kako doseči visoko učinkovitost predlaganih rešitev.

Iztok Saje se je z radiom spoznal kot mlad radioamater (S52D). Od leta 1992 se v Mobitelu ukvarja z načrtovanjem, gradnjo in optimizacijo mobilnih omrežij. Sedaj je strateg v Sektorju za dostopovna omrežja v Telekomu Slovenije. Iztok je tudi predavatelj na VSŠ za telekomunikacije v Ljubljani.

Vzpostavitev operacijskega centra za nadzor in upravljanje informacijskih varnosti v kritični infrastrukturi

Boštjan Gruden, Boštjan Mencigar, Miha Mesojedec, FMC, Ljubljana

Povzetek — V članku predstavljamo strukturo varnostnih sistemov in izzivov, s katerimi se ti sistemi soočajo danes. Poudarek je na preoblikovanju sistemov SIEM v centralni živčni sistem za obsežne varnostne analize, ki vključuje natančno vidljivost, globljo analitiko, veliko razširljivost, akcijo in enoten pogled.

Ključne besede — varnostni ekosistem, SIEM, Security Analytics, SOC, CIRC

Abstract — This article presents the structure of security systems and challenges they face today. It emphasises the transformation of SIEM systems into a central nerve system for extensive security analyses that include active monitoring, deep analysis, expansion and multi-lever architecture, action and single view

Keywords — security ecosystem, SIEM, Security Analytics, SOC, CIRC

I. VARNOSTNI EKOSISTEM

Varnostni sistem je varen toliko kot je šibek najmanjši člen v sistemu. Če naredimo vrhunski »setup« na enem delu, pa pademo na nekem drugem dogodku, ki je sicer manjšega pomena ali ga vidimo kot nepomembnega, in če nato ne poskrbimo za ta dogodek, nam vse ostalo kaj veliko ne pomaga. Vsak, ki se nas bo želel lotiti, nas bo napadel tam, kjer smo najbolj ranljivi. Takšen ekosistem je izredno pomemben, ne samo zato, da vemo kako funkcionira, ampak da lahko tovrstne dogodke zaznamo in čim prej začnemo z njegovim reševanjem.

II. VARNOSTNA ANALITIČNA PLATFORMA

V zadnjih letih je veliko korporacij podleglo organiziranim kibernetskim napadom. Povsem jasno je, da trenutni varnostni sistemi niso kos nalogi preprečevanja naprednih groženj, saj večina omrežij vsebuje sisteme za odkrivanje in preprečevanje vdorov, ki temeljijo na vnaprej znanih napadih. Takšni sistemi ne zmorejo zaznati t. i. APT (»Advance Persistent Thread«) napadov, ker so le ti fokusirani in pripravljeni specifično za neko okolje. Glede na današnje grožnje, povečevanje dostopnosti in povezljivosti v digitalni infrastrukturi, se varnostne ekipe zavedajo, da so njihova okolja nenehno ogrožena. Varnostnim sistemom kot jih poznamo danes, se dnevi počasi iztekajo. Potrebujemo nove prakse, ki temeljijo na razumevanju faz napada, nenehnem spremljanju in hitrem odkrivanju groženj.

Razvoj prepoznavanja, agilnost in hitrost spopadanja s sodobnimi grožnjami tradicionalno temelji na varnostnih strategijah za spremljanje, ki običajno bazirajo na sistemih za upravljanje varnostnih informacij in dogodkov (»SIEM«). Ti sistemi se morajo iz tradicionalnosti razviti v centralni živčni sistem za obsežne varnostne analize in morajo vsebovati štiri temeljne funkcionalnosti:

A. Natančna vidljivost

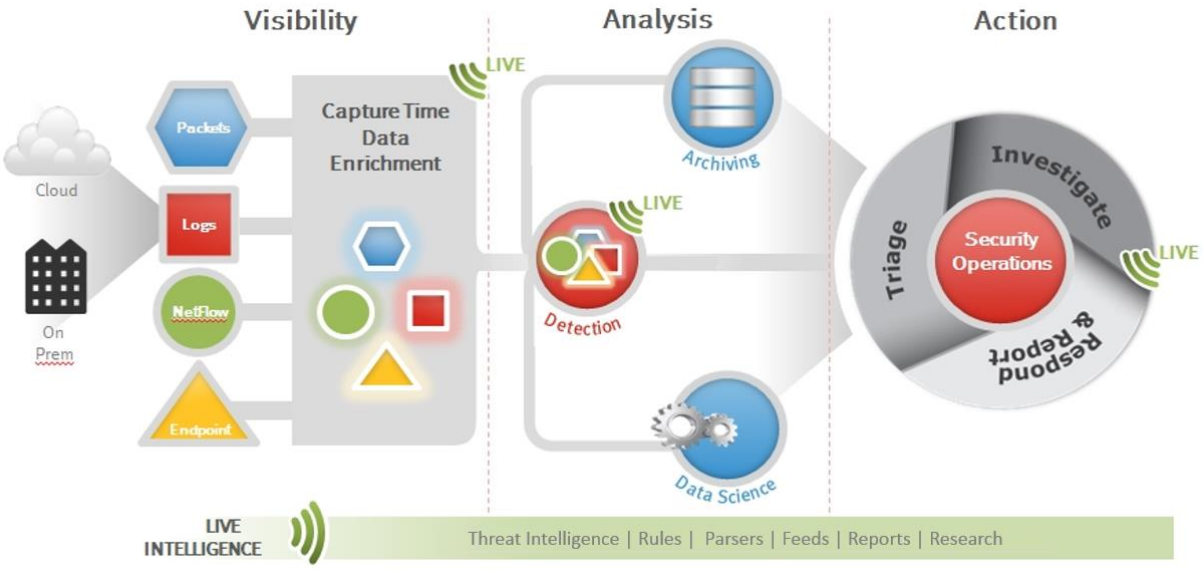
Preden lahko organizacije ustavijo »nevidne« kibernetične napade, morajo najprej imeti možnost, da jih vidijo. Varnostna analitična platforma v celoti zagotavlja polno rekonstrukcijo aktivnosti ter omogoča varnostnim analitikom odločanje ob razpoložljivih informacijah in pravilen odziv ob morebitnih težavah. Mrežno zajemanje paketov in rekonstrukcija sej v naslednjo generacijo SIEM sistemov je bistvenega pomena za varnostne analitike, da raziščejo sodobne grožnje. Tradicionalni SIEM sistemi lahko podajo informacijo, da je nek računalnik komuniciral z zlonamernim strežnikom, vendar pa ne vedo, katere informacije so bile odtujene. Prav tako je pomembna analiza NetFlow in »EndPoint« informacij, saj s tem zajamemo celotno omrežje in vse končne naprave v nekem okolju.

B. Globlja analitika

Preučevanje tveganj in kontekstov s primerjavo različnih vzorcev izboljša razmerje detekcije med pravimi in lažnimi grožnjami ter tako pospeši čas reševanja in odkrivanja napadov. Varnostni sistemi za analitiko morajo iskati vedenjske vzorce in dejavnike tveganja ter se ne smejo osredotočati na statična pravila in znane podpise. Napredna analitika poudarja dogodke, ki zahtevajo podrobnejši pregled. Samodejni inteligentni analitični sistemi so pomemben del nove varnostne analitične platforme, vendar ne prevzemajo mesta človeški presoji, temveč le izpostavijo območja, kjer je človeška presoja nujna.

C. Velika razširljivost

Platforme za zbiranje velikih količin varnostnih podatkov morajo biti razširljive v velikem obsegu, da lahko shranjujejo množične količine informacij, ki so čedalje bolj potrebne za popolno situacijsko zavedanje. Globlji vpogled v prometne tokove iz številnih mrežnih naprava po omrežju povečuje količino podatkov, katere morajo analitične platforme obravnavati. Za spopadanje z današnjimi grožnjami je potrebno zagotoviti funkcionalnost distribuirane več nivojske arhitekture za shranjevanje podatkov ter analitični proces, ki normalizira in procesira veliko različnih podatkov z zelo visokimi lastnostmi.



Slika 1: Proces prepoznavanja in spopadanja z grožnjami

D. Akcija

SOC (Security Operation Center) okolja so običajno preobremenjena z velikimi količinami podatkov in opozoril, zato je še posebej težko odkriti, razlikovati in sprejeti ciljno usmerjene ukrepe na najpomembnejših incidentih.

Sistem mora omogočati:

- Prioriteto preiskav in racionalizacijo več hkratnih analitičnih potekov dela v enem orodju.
- Predpostavimo, da je vsak incident samo vrh ledene gore. Če želimo pridobiti več informacij, lahko izvedemo preiskavo (»pivot«) preko ustvarjenih incidentov v spletnem vmesniku, kjer pridobimo več informacij glede končnih točk (»endpoint«), mrežne forenzike prometa, malware analize, NetFlow prometa in dnevniških zapisov, ter šele nato razumemo pravi obseg posameznih incidentov.
- Vgrajene najboljše SOC prakse s katerimi lahko učinkovito upravljamo SOC orodje in z njim usposabljamo varnostne analitike.

E. Enoten pogled

Za popolno obveščenost in pregled dogodkov analitiki potrebujejo varnostne informacije na enem mestu, saj so te ključnega pomena za preiskovanje incidentov in hitrejše odločanje o morebitnih grožnjah.

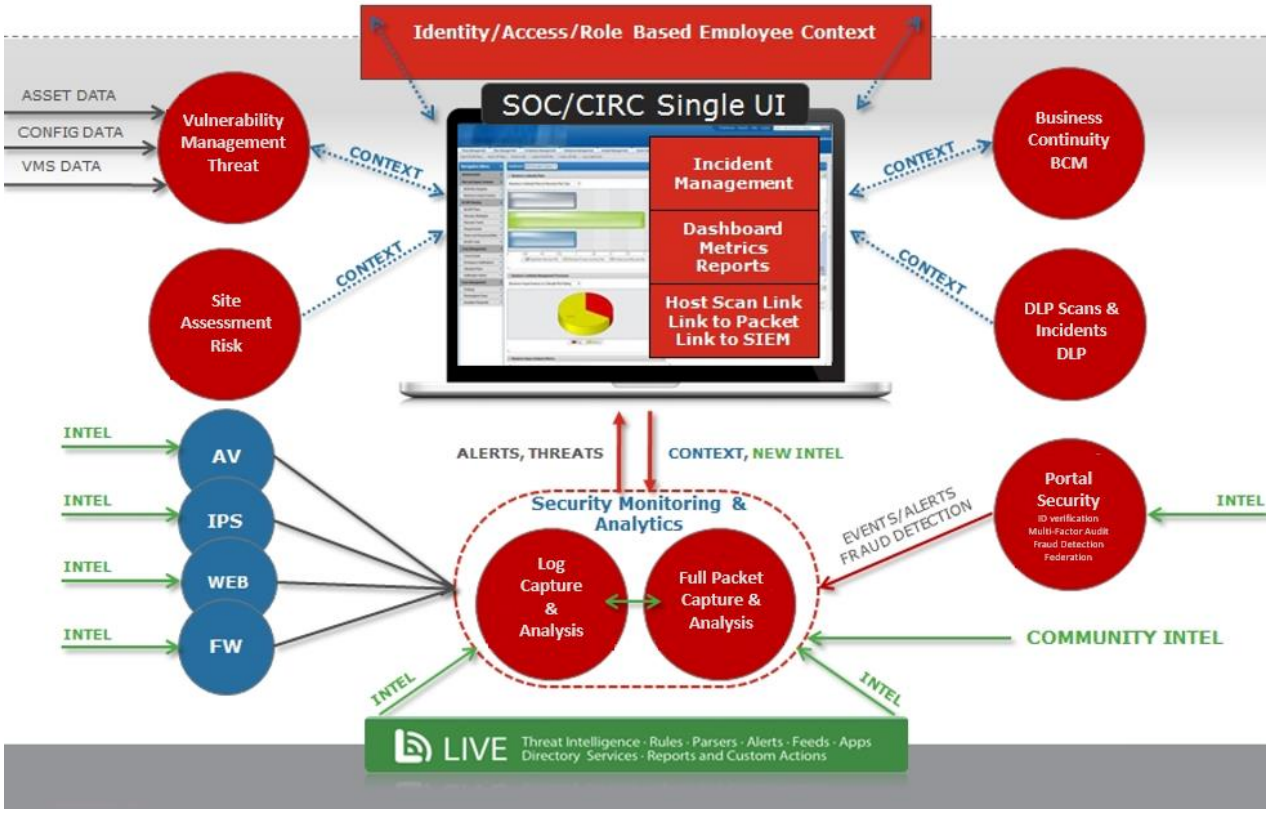
Kot odgovor na ta vprašanja so v nenehnem razvoju novo skalabilna orodja ekosistema. Visoko skalabilna platforma omogoča sprejemanje velikih količin podatkov („Big Data“) ter nad njimi opravlja analitično analizo. Taka platforma mora vsebovati vse običajne funkcije SIEM sistemov z možnostjo nadgradnje analize omrežnega prometa. Za shranjevanje velikih količin podatkov se običajno uporablja Hadoop tehnologija. Analitična orodja morajo zagotavljati učinkovito preiskovanje, analizo zlonamerne kode, poročanje in zmožnost opozarjanja. Dodatno vrednost celotni arhitekturi varnostnega ekosistema dajejo viri zunanjega znanja. Te informacije se pridobi od globalnih naprednih organizacij, ki se ukvarjajo z raziskovanjem in analizo napadov, javnih skupnosti in ostalih virov. Informacije so nato integrirane v sistem na način pravil, opozoril, filtrov … Komponenta upravljanja mora zagotavljati skladnost, upravljanje incidentov ter v kasnejših implementacijah aktivno obrambo. Platforma na tak način omogoča tudi integracijo z ostalimi varnostnimi in informacijskimi sistemi, kar le še povečuje dodano vrednost samega sistema in omogoča varnostnim ekipam poenoten vpogled nad celotnim omrežjem.

Namenska platforma za SOC, ki vsebuje najboljše prakse (»Veris Framework«, NIST US-CERT, CIRC), postavlja okvirje za uspešno delovanje SOC in združuje ljudi, procese in tehnologijo v enotno platformo, s katere je možno upravljati varnostne grožnje naslednje generacije. Sama platforma mora omogočati združevanje velike količine dogodkov iz različnih sistemov in nato nad njimi izvajati različne operacije, kot so »Incident Response«, »Brach Response« in »SOC Program Management«. Vsebovati mora tudi prilagojeno nadzorno ploščo in poročanje.

Pri orodju za odkrivanje malware napadov na končnih točkah (»endpoint«) se uporablja popolnoma nova metoda, ki ne temelji na predpisanih podpisih (»signature«), ampak na analizi vsebine računalnika (disk, gonilniki, kernel ...), trenutnega stanja spomina (»RAM«) in analize mrežnega prometa. Vsebovati mora tudi IOC (Indicators of Compromise) in YARA prakse, s katerimi se odkriva zlonamerne aktivnosti

III. PRIMER EMC CIRC

EMC CIRC (Critical Incident Response Center) uporablja EMC in RSA tehnologije za osrednji nadzor in zaščito EMC-jevih operacij po svetu, ki vključujejo več kot 60.000 ljudi, 400 korporativnih in prodajnih pisarn ter množico partnerjev v več kot 85 držav po svetu.



Slika 2: Struktura sodobnega varnostnega ekosistema

A. *Zaščititi globalno organizacijo*

EMC je vodilno podjetje na svetu za informacijsko infrastrukturo. Njegove stranke prihajajo iz vseh gospodarskih panog v privatnem in javnem sektorju in so različnih velikosti, od startupov do članov Fortune Global 500. Naši kupci so globalne velike banke in druga vodilna podjetja na področju finančnih uslug, industrija, organizacije s področja zdravstva in znanosti o življenju, ponudniki telekomunikacijskih in internetnih storitev, letalske družbe in transportna podjetja ter izobraževalne ustanove in agencije javnega sektorja. Podjetje zaposluje 60.000 ljudi po vsem svetu, pri čemer jih več kot 40 odstotkov dela izven ZDA, in tesno sodeluje z globalno mrežo partnerjev s področja tehnologije, „outsourcing"-a, sistemskih integracij, storitev in distribucije.

Kot pri večini velikih podjetij, se EMC vseskozi sooča z vedno večjimi izzivi kako zaščititi svoje zaposlene, stranke, objekte in informacijska sredstva od vedno večjega spektra naprednih groženj.

B. *Prilagajanje varnosti poslovnemu tveganju*

Da bi se lažje soočal z dinamično naravo groženj, EMC teži k stalnemu izboljševanju svoje varnostne strategije kot tudi organizacije, ki jo podpira. Pri zaščiti svojega poslovanja podjetje ni več vezano na neodvisne varnostne naprave in varnostne ekipe, ki delajo v izoliranih okoljih. Danes EMC potrebuje celovit pogled na podjetje - tako fizični kot digitalni - za boljše razumevanje dogodkov in trendov v celotnem podjetju, ki bi lahko vplivali na njegove rizične in poslovne operacije.

Da bi to dosegli, je EMC postavil enotno varnostno organizacijo, ki vključuje Pisarno za informacijsko varnost (Office of Information Security), Storitve korporativne zaščite (Corporate Protective Services), Odzivni center za kritične dogodke (Critical Incident Response) in Skupine za vzpostavitev poslovne varnosti (Business Security Enablement group). Z združitvijo teh organizacij pod eno streho je EMC sposoben identificirati matrike in trende na vseh področij, kar mu omogoča celovit pregled na tveganjem v celotni organizaciji. Na primer, če ekipa oddelka za Storitve korporativne zaščite identificira večje število kraj intelektualne lastnine, lahko skupina Pisarne za informacijsko varnost uporabi te informacije za vzpostavitev nadzornih mehanizmov, s katerimi bodo preprečene bodoče kraje intelektualne lastnine.

C. *Specializacija za odkrivanje*

Kot del te strategije je EMC postavil „Critical Incident Response Center" (CIRC), naslednje-generacijski varnostni objekt, ki združuje podatke o poteku dela in kjer so povezana različna področja organizacije, varnostne naprave in tehnologije, kar omogoča enoten pregled nad spremljanjem in izvrševanjem EMC-jevih globalnih operacij.

CIRC je bil postavljen z uporabo tehnologij in najboljših praks, ki jih je razvil RSA, in se napaja z več kot 2.000 varnostnih naprav, ki ustvarjajo od 12 do 14 milijonov varnostnih dogodkov na uro na svetovni ravni.

V CIRC-u se specializirana, več funkcionalna in visoko izurjena ekipa osredotoča na spremljanje kritičnih groženj in odzivanj na izredne dogodke ter izvaja naslednje storitve za podjetje:

- aktivno spremljanje varnostnih sistemov za sumljivo ali znano obnašanje,
- situacijske in poslovne analize identificiranih nevarnosti za organizacijo,
- „triaža" / zajezitev in usklajevanje kritičnih incidentov po vsem podjetju,

– zbiranje obveščevalnih podatkov in informacij o grožnjah od notranjih in zunanjih virov.

Pred dvema letoma je bil CIRT re-aktivna, „eyes on glass“ operacija. Ko je EMC ocenjeval svoje strateške možnosti za razvoj operacij, je vdor v RSA v marca 2011 pospešil proces, v katerem je EMC razširili zmogljivosti in strokovno znanje CIRC-a na področju naprednih orodij, taktike in analize (ATTA) ter analize podatkov in vsebin spletnih groženj.

Pokazano na primeru malware se proces začne z „eyes on glass“ varnostno analizo v CIRC-u, kjer se iščejo anomalije in kazalci kompromitiranosti. Po identifikaciji kosa zlonamerne programske opreme kot dela incidenta, se le-ta izroči ATTA skupini za nadaljnjo analizo in razčlenitev. Ko je malware obratno inženiran in so opredeljeni njegovi atributi, bo skupina za analizo podatkov spletnih groženj raziskala kazalnike in jih navskrižno preverila z obstoječimi informaciji ter dodala profil malware podatkovni bazi. Od tod se informacija prenese do ekipe za vsebine spletnih groženj v namen ustvarjanja poročil, novih pravil ali opozoril ter integracije v obstoječe komplete orodij. Na ta način se ob pojavu podobne grožnja le-ta takoj označi za analizo v CIRC in se sklene informacijska zanka.

Te skupine danes z zbiranjem informacij in indikatorjev kompromitiranosti, ki omogočajo analitikom CIRC-a hitrejše odkrivanje anomalij, tudi omogočajo EMC-ju večji manevrski prostor in proaktivno odkrivanje naprednih groženj. S takšnim enotnim in integriranim vpogledom nad globalnim podjetjem, lahko analitiki CIRC-a dajejo nasvete in napotke EMC in RSA menedžmentu glede zaznavanja varnosti, odzivanja in sanacije, ki temeljijo na preverjenih informacijah.

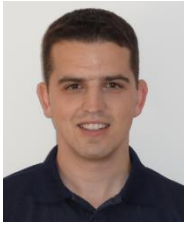
LITERATURA

[1] RSA ADVANCED SECURITY OPERATIONS CENTER SOLUTION, http://www.emc.com/collateral/data-sheet/h13413-ds-pdf-rsa-soc-overview.pdf

[2] THE EMC CIRC, Protecting the enterprise by hunting and detecting unknown cyber threats

Boštjan Mencingar je direktor podjetja FMC, članice Skupine FMC d.o.o.

Boštjan Gruden je generalni menedžer podjetja Miška d.o.o., članice Skupine FMC d.o.o.



Mag. **Miha Mesojedec** je RSA konsultant za Vzhodno Evropo.

Command Center Solution to organize workforce and resources (real case presentation of Swiss organisation)

Michael Bausback, Logobject, Zurich

Abstract — This article explains importance of trends recognition in daily business. Critical infrastructure needs special care from agile service organizations. Process model described in details in this paper is mainly used in Telco and IT industry. It comprises of three modules: (1) Workforce management, (2) Complex order handling and (3) Asset tracking module.

Keywords — Service Chain, Process, Technology, Quality, ROI, Logistics, Workforce Management, ITIL, eTOM, SLA

IV. Introduction

In today's time it is important to recognize trends early on and to move them sensibly and economically into profit driven businesses. Critical infrastructure needs maintenance by fast moving and agile service organizations with a state of the art planning and control application. Our company is providing this for logistics processes mainly to increase productivity for service organizations and their work order management. Target industries are all service providing organizations in particular: Telecommunication, White Goods, Document Management and Office Equipment Suppliers.

V. Industrialization of Service Chains

Service quality is a deciding value driver for the Telecom industry. Especially in price dominated markets service levels play a major role. On the buy side when customer decisions are influenced by service quality. On the sell side when service optimization leverages total ROI.

Service improvement is a natural goal in every business. The challenge is to manage services in a way to make them pay off. The solution remains in adjusting the complete service chain. Workforce management (WFM) must focus every single process and requires automation to achieve maximum efficiency.

A. *Secure Service for Critical Infrastructure*

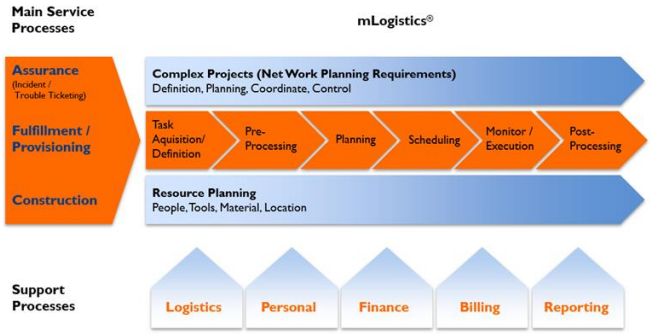
Real time decisions based on the actual availability of resources allow immediate reaction by at the same achieving the best possible use of resources. Field force can be directed to a next service job via mobile communications immediately when a situation arises.

B. *Service perfection to meeting SLA's*

- Real time information about production progress, orders and utilization of the employees.
- Reducing lead times as well as inventory and logistics costs.
- Efficiency increase in the execution of the operational processes.
- Real time dispatching and monitoring of all resources.
- Transparent proof of performance of every resource.
- Increasing on-time delivery quality.
- Providing preventive maintenance capabilities.
- Real time synchronization from and between in-house and remote business processes.
- Transparent communication with customers.

VI. mLogistics Processes and Technology

The business process model is related to proven concepts like the eTOM and ITIL models used in the Telco and IT industry respectively. This ensures transparent use in critical infrastructure organisations.



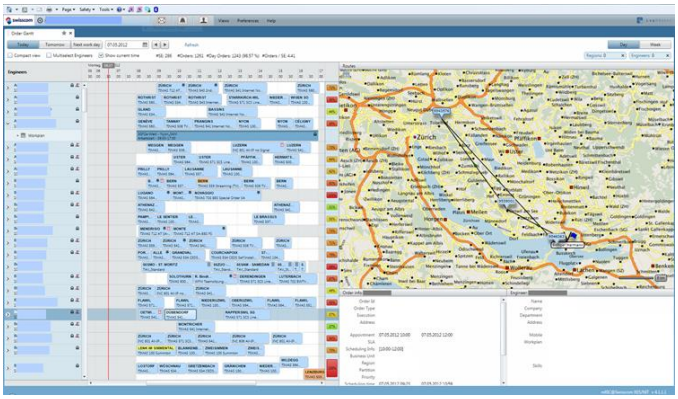
Picture 1: mLogistics process

mLogistics is built as a standard product comprising of 3 main modules: Work Force Management, Complex Order Handling and Asset Tracking.

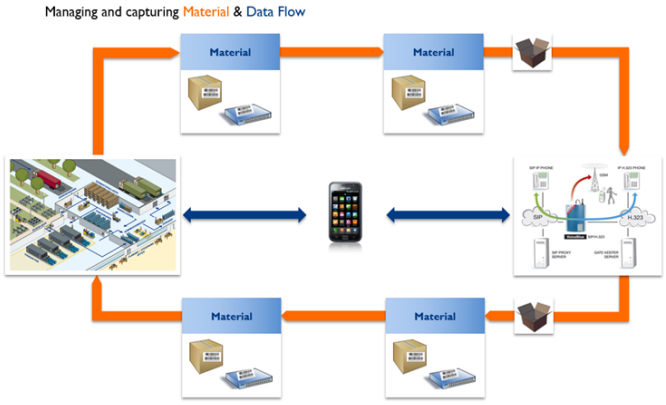
A. *Work Force Management*

The flow of task processing with *mLogistics* is illustrated in the entire handling of an order, from the capture over pre-processing, planning, scheduling, dispatching, execution and post-processing. The System is browser based with easy navigation using standard workspaces and favourites to allow easy adaption to each work process.

A comfortable user interface with GANTT chart grants easy overview (tasks and geographies) for dispatchers allowing drag and drop to assign as well fully automatic scheduling.



Picture 2: Work Force Management



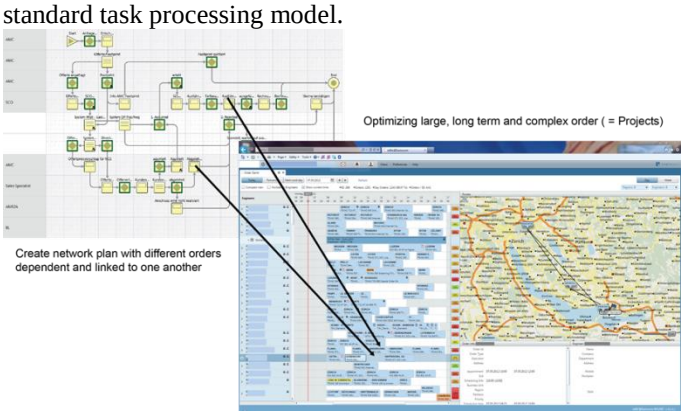
Picture 4: Asset tracking and logistics

B. *Complex Order Handling*

mLogistics enables users such as project managers or dispatchers in the back office to manage, plan and execute complex orders: Generally complex orders consist of multiple "simple tasks" organized in a complex network of dependencies. In *mLogistics* the following definition is used:

- Complex orders are called projects.
- Simple orders are called tasks.

Due to the fact that a project consist of a set of tasks whose dependencies are governed by a defined network, the processing of tasks contained within a project follow the standard task processing model.



Picture 3: Complex order handling

C. *Asset Tracking and Logistics*

The vehicles are administered as a warehouse (Van stock). To administer a warehouse *mLogistics* must directly control every receipt and usage of material in the warehouse. This process allows controlling and maintaining a complex infrastructure by keeping track of changes. These processes can be triggered automatically from preventive maintenance tasks.

D. *Software Architecture and Components*

mLogistics is a 3-tier application. The system architecture is based on a bus, where new processes or interfaces can be integrated simply and quickly. Therefore the system ensures a high degree of future security and upgradability as all components correspond on recent industry standards. Automated client distribution mechanism is also integral part of *mLogistics*, so that the operation effort can be radical optimized.

In the latest release the system supports all 3 major mobile platforms: Android, iOS and Windows Phone.

Michael Bausback is Swiss citizen, born in Germany. He is IT veteran. He has worked for 25 years in large IT organisations, 20 of these with IBM in different countries (Germany, South Africa, and Switzerland). Other assignments were Xerox, Commerce One, mainly in sales and business development roles. Since 10 years he has been with LogObject AG developing the company from a project oriented company to a product house with a strong standard product.

Napredne rešitve za varnost v cestnem prometu

Ana Robnik, Gorazd Novak, Iskratel, d.o.o., Kranj

Povzetek — Varnost v cestnem prometu na sistemskem in družbenem nivoju je pomembna kategorija v politiki Evropske unije. Ukrepi za izboljšanje varnosti cestnega prometa vključujejo tehnologije inteligentnih prometnih sistemov, med njimi igrajo pomembno vlogo telekomunikacijske tehnologije. Storitev s tega področja je »Klic v sili za vozila (eCall)«, za katero Evropska komisija zagotavlja, da bo v celoti operativna od 1. oktobra 2017 dalje. Podjetje Iskratel je s svojo inovativno rešitvijo za to področje, imenovano eCall Node, in s svojo usmeritvijo na področje naslednje generacije storitve 112 pomemben igralec na tem področju, tako v evropskem kot tudi drugih trgih.

Ključne besede — varnost v cestnem prometu, eCall, storitev 112, PSAP, eCall Node, nevarne snovi, težka tovorna vozila, VITEL

Abstract — Road traffic safety at system and societal levels is an important category in the European Union policy. Measures to improve road safety include intelligent transport systems technologies, among them telecommunications technologies play an important role. The eCall service has been mandated by the European Commission to be fully operational service by the 1st of October 2017. Iskratel positions as a major player in this field with its innovative solution entitled eCall Node and with its orientation towards the next-generation 112 service, both on the European and foreign markets.

Keywords — road traffic safety, eCall, 112 service, PSAP, eCall Node, hazardous goods, heavy goods vehicles, VITEL

I. UVOD

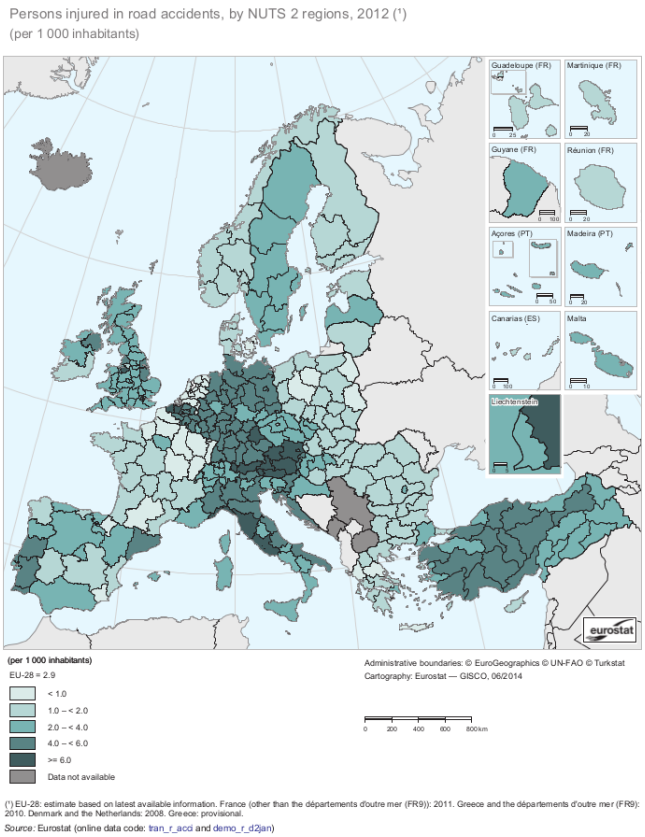
Cestni promet, kot najbolj razširjeno obliko kopenskega prometa v Evropski uniji, v svoji politiki naslavlja Generalni direktorat za mobilnost in promet pri Evropski komisiji [1]. Kaj želi doseči Evropska unija s politiko cestnega prometa je opisano v brošuri [2], kjer so na koncu zbrani tudi glavni dokumenti (smernice, predpisi, standardi, …) s tega področja.

V pomembnem dokumentu Evropske komisije iz leta 2011 z naslovom »BELA KNJIGA, Načrt za enotni evropski prometni prostor – na poti h konkurenčnemu in z viri gospodarnemu prometnemu sistemu« [3] je opisana priprava evropskega prometnega prostora za prihodnost ter vizija in strategija za konkurenčen in trajnosten prometni sistem. V njem je poudarjeno, da morajo sofinancirani projekti oddražati zapisano vizijo in strategijo in bolj poudarjati evropsko dodano vrednost. V dokumentu je tudi zapisnao, da morajo sofinancirani projekti enako odražati tudi potrebo po infrastrukturi (cestni, informacijsko-komunikacijski), ki ima čim manjši vpliv na okolje, je odporna na morebitne učinke podnebnih sprememb ter izboljšuje varnost in zaščito uporabnikov. Poleg tega navaja tudi promocijo evropskih standardov na področju varnosti, zaščite, zasebnosti in okolja.

Varnost v cestnem prometu je pomemben ekonomski in sociološki dejavnik, kajti okrog 44 % blaga v EU prevažajo po cesti, ljudje največ potujemo v osebnih vozilih, kar predstavlja 73 % potniškega prometa, cestni promet pa je pomemben gospodarski sektor sam po sebi, ker zaposluje približno 5 milijonov ljudi po vsej EU in ustvarja skoraj 2 % BDP [2].

II. UKREPI ZA POVEČANJE VARNOSTI

Evropska komisija je objavila predhodno poročilo s podatki o varnosti v cestnem prometu za leto 2014 [4]. V njem je omenjeno, da se skupno število umrlih na cestah EU k sreči zmanjšuje, vendar žal ne v vseh državah. Prav tako slabše sledimo cilju do 2020, ko naj bi se to število razpolovilo glede na leto 2010, ko je ugasnilo življenje 31.500 ljudi. Razveseljiv je podatek za Slovenijo, kjer je bilo to število v letu 2014 za 15 % manjše kot v predhodnem letu. Slika prikazuje podatke o poškodovancih nesreč v cestnem prometu na 1000 prebivalcev v regijskih enotah EU na drugem nivoju za potrebe statistike (NUTS 2 – Nomenclature of Territorial Units for Statistics Level 2). Podatki so sicer iz leta 2012. Za Vzhodno regijo v Sloveniji in naše neposredne sosede, predvsem Avstrijo, so podatki zaskrbljujoči.



Slika 1: Porazdelitev števila ranjenih v prometnih nesrečah na 1000 prebivalcev (vir: Eurostat 2012)

Vsako življenje je dragoceno, ob takih številkah pa je potrebno še posebej pozorno načrtovati ukrepe. Zato je Evropska komisija novembra 2012 predložila akcijski načrt CARS 2020 [5] in po dveh letih je ekspertna skupina, vključujoč javno mnenje, zaključila proces CARS 2020 in podala poročilo [6]. V njem je zapisana zaveza Evropske komisije, da še naprej spodbuja uvajanje inteligentnih

prometnih sistemov, posebej še vseevropskega sistema Klica v sili v vozilih »eCall«. Uveljavijo se ustrezni zakonodajni ukrepi za zagotovitev močnega usklajevanja ter pravočasne in popolne postavitve vseh potrebnih elementov, povezanih s sistemom eCall. Tako bo sistem za reševanje življenj učinkovito deloval v letu 2015. Ne nazadnje, Evropski svet in Evropski parlament sta se strinjala, da morajo države članice na svojem ozemlju zagotoviti vse potrebno, da sistem eCall v celoti implementirajo do 1. oktobra 2017, kar pomeni tudi ustrezno nadgradnjo sistemov za sprejemanje klica v sili, tako imenovanih sistemov PSAP (Public Safety Answering Point).

Direktiva ITS (Direktiva 2010/40/EU) določa pravni okvir za uvajanje medobratovalnih, združljivih in trajnih sistemov in storitev inteligentnih prometnih sistemov po vsej Evropi. Prednostni ukrepi c, d, e in f v tej Direktivi vključujejo tudi "zagotavljanje vseevropske storitve eCall".

III. STORITEV ECALL REŠUJE ŽIVLJENJA IN ZMANJŠUJE STROŠKE

A. Na kratko o storitvi eCall

Ker je bil osnovni sistem Klica v sili za vozila (eCall) na delavnici VITEL že predstavljen [7], na tem mestu opišimo le osnovne principe, povezane s samo storitvijo eCall.

Storitev eCall je vseevropska storitev, na voljo v vseh novih in nadgrajenih obstoječih vozilih, ki temelji na enotni evropski številki za klic v sili 112. Storitev eCall je storitev javnega ali zasebnega značaja. V prvem primeru to storitev zagotavljajo nadgrajeni centri PSAP, v drugem pa organizacije kot so avto-moto zveze in druge zasebne organizacije. Obe storitvi hkrati delujeta, bodisi ločeno ali v sožitju z medsebojnim dopolnjevanjem.

Storitev eCall v vozilu je glasovna storitev 2G-omrežja, ki v delu vsebine govornega kanala prenaša tudi minimalno zbirko podatkov (a Minimum Set of Data - MSD), povezanih z nesrečo, v kateri je bilo udeleženo to vozilo. Med najpomembnejšimi podatki so natančna lokacija, čas in smer vožnje. Storitev eCall se lahko proži ročno ali v večini primerov samodejno na podlagi kriterijev, ki nek dogodek razpoznajo kot dogodek v sili. Klic v sili sprejme najbližji center 112 in ga obdela kot vsak drugi klic v sili. Storitev eCall deluje skladno z regulacijo na področju zasebnosti in zaščite podatkov. Storitev eCall uporablja skupne evropske in svetovne standarde, ki sta jih definirali standardizacijski organizaciji ETSI in CEN.

B. Storitev eCall rešuje življenja

Analize kažejo, da storitev eCall lahko zmanjša odzivni čas na storitve v izrednih razmerah do 50 % na podeželju in do 40 % v urbanih področjih, kar vodi k zmanjšanju števila umrlih v nesrečah med 2 in 10 % ter k zmanjšanju resnosti poškodb in poškodovancev med 2 in 15 %. Ta razpon je v veliki meri odvisen od držav, kjer so izvajali te analize.

C. Ostali pozitivni učinki storitve eCall

Storitev eCall bo pohitrila reševanje izrednih razmer v naslednjih okoliščinah:

- udeleženci v trčenju so lahko nezavestni, v šoku ali ne morejo vzpostaviti stika z reševalci,
- trčenje se zgodi na podeželju ali na redko naseljenih področjih (največ nesreč s smrtnim izidom se zgodi na podeželskih cestah in poteh),
- v trčenju je udeleženo le eno vozilo (po statistikah 40 % ljudi umre v nesrečah, kjer je v vozilu le voznik),
- udeleženci in očividci ne morejo sporočiti ali določiti lokacije nesreče oziroma trčenja (predvsem na medkrajevnih cestah in med potovanjem v tujini),
- trk oziroma nesreča se dogodi v nočnem času.

Kot sledi iz povedanega, ima storitev eCall največji učinek na oddaljenih področjih in ponoči. Podnevi je na prometnih cestah njena uporabna vrednost za prepoznavanje cestnih zastojev in preprečevanje trkov. Storitev eCall bo koristila potnikom, ki potujejo v tujino in se slabše znajdejo v tujih razmerah in težje prepoznavajo točno lokacijo.

Storitev eCall ima pozitiven učinek tudi na okolje in na ostale udeležence v prometu. Zaradi hitrejšega prihoda na kraj nesreče so njene posledice tudi prej odpravljene, kar pomeni manjše tveganje verižnih nesreč in posledično daljših zastojev. Pri tem se občutno zmanjša poraba goriva in izpušnih plinov ter poveča prijaznost okolju.

Storitev eCall ima posebno velik učinek v primeru, ko je v nesreči udeleženo vozilo, ki prevaža nevarne snovi. Vsak dodatni podatek o samem tovoru in kraju nesreče lahko občutno zmanjša negativen vpliv na soudeležence in na okolje.

Veliko drugih organizacij, kot so avtomobilska združenja, zavarovalnice in proizvajalci avtomobilov, imajo prav tako pozitivne učinke ob uporabi storitev eCall.

Izraženo izključno v grobih finančnih okvirih, kajti vsako življenje je neprecenljivo, znaša ekonomska izguba v EU zaradi prometnih nesreč več kot 160 milijard € na leto. Če bi bili vsi avtomobili opremljeni s sistemom eCall, bi lahko letno prihranili do 20 milijard €, kar predstavlja 12,5 % vseh stroškov.

IV. ISKRATELOVA INOVATIVNA REŠITEV ZA PODPORO STORITVI ECALL

A. Iskratel - podjetje s tradicijo in naprednimi rešitvami za centre 112

Iskratel ima dolgoletno tradicijo v pripravi rešitev za centre 112 oziroma centre za izredne razmere. V svojem portfelju rešitev ima za to področje na voljo rešitev, ki vsebuje storitve in aplikacije, ki omogočajo natančno izmenjavo informacij in koordinacijo ekip, ki sodelujejo v intervencijah.

Rešitev se imenuje »Emergency Services Suite«, njen ključni del pa “Emergency Communication and Information System”, ki omogoča učinkovito organizacijo intervencij, tudi na terenu, in odstranitev posledic incidentov. V ta namen se uporabljajo glasovne in podatkovne komunikacije (faks, elektronska pošta, neposredno sporočanje), ki so dopolnjene z enostavnimi video komunikacijami in storitvami za učinkovito medsebojno sodelovanje.

B. eCall Node – rešitev za storitev eCall

Storitev eCall oz. sistem eCall temelji na ustrezni funkcijski razširitvi centrov 112 in na dodatnem vozlišču, ki smo ga poimenovali »eCall Node«. Le-ta je vmesni in vezni člen med napravo v vozilu, ki proži govorni klic do centra 112, in med centrom 112. Vsi klici so torej preusmerjeni na to vozlišče, ki je sposobno iz vsebine govornega kanala izločiti minimalno zbirko podatkov (MSD) in dane podatke po ločenem podatkovnem kanalu poslati najbližjemu oz. najprimernejšemu centru 112 ali jih preusmeriti na drug center oz. hkrati poslati na druge pomembne ponorne točke za različne namene, skladno z regulacijo in zakonodajo.

Rešitev smo izdelali v več fazah, in sicer smo:

– raziskovalno fazo s preizkusom koncepta za eCall Node v povezavi z razširjenim centrom 112 zaključili v okviru 2. faze projekta HeERO II [8], kjer je bila Slovenija kot država pridružena članica projekta,
– raziskovalno fazo s preizkusom koncepta izmenjave podatkov med javno in zasebno storitvijo eCall izvedli v okviru raziskovalnega projekta z imenom »Usklajeni eCall«,
– razvojno fazo in produktivizacijo dosežkov raziskovalnih projektov rešitve eCall Node zaključili v okviru internega razvojnega projekta.

V evropskem projektu HeERO II [8] je bila prijavitelj in uradno sodelujoča organizacija na projektu Uprava RS za zaščito in reševanje, podjetji Iskratel, d.o.o. in Telekom Slovenije, d.d. pa njena tehnološka partnerja.

V nacionalnem projektu eCall4All so poleg našega podjetja, kot nosilca in koordinatorja projekta eCall4All, sodelovali s svojimi deli rešitve še podjetja Alpineon, d.o.o., AMZS, d.d., Telekom Slovenije, d.d., IPKOM, d.o.o. in javna raziskovalna organizacija Fakultete za računalništvo in informatiko Univerze v Mariboru.

V. STORITEV ECALL V SLOVENIJI

A. *Izzivi pri izvedbi*

V 1. in 2. fazi projekta HeERO so se države [11] soočale z naslednjimi izzivi pri izvedbi sistema eCall:

– zaradi zmanjševanja stroškov v državnih organih in zaradi zamika zakonske obveze uvajanja storitve eCall, njena izvedba običajno ni prednostna naloga. Naložbe se pričakujejo v terminih, ki so povezani z zakonskimi obligacijami. Prav tako je zaželeno njeno preprosto, hitro in cenovno učinkovito uvajanje.
– zmogljivostjo in govornimi kanali, kajti realno je pričakovati, da bo število klicev v sili eCall vztrajno naraščalo s časom, kar zahteva od rešitve ustrezno prilagodljivost na povečane kapacitete in enostavno razširljivost.
– v določenih okoliščinah prihaja do preobremenitev v centrih 112 in nadzornih sobah. V takih primerih je izjemno dobrodošla rešitev, ki vključuje uravnoteženo delovanje celotnega sistema, kar vključuje usmerjanje do različnih centrov 112 in usmerjanje na podlagi izkušenj do različnih skupin operaterjev.

Na podlagi zgoraj omenjenih izzivov in proučitve naših realnih danosti smo se v Sloveniji odločili za centralizirano rešitev na podlagi rešitve eCall Node.

B. *Arhitektura rešitve*

Srce rešitve je centraliziran eCall Node, kamor se usmerjajo eCall govorni klici z vgrajenimi podatki MSD.

Za ta namen se uporablja zaznamek eCall, ki omogoča razlikovanje med mobilnimi klici 112 in klici eCall. V dani rešitvi so glavne funkcije vozlišča »eCall Node« naslednje:

– demodulacija vgrajenega signala MSD s pomočjo integriranega podatkovnega modema eCall,
– dekodiranje MSD,
– analiza podatkov v MSD in
– inteligentno usmerjanje klica in podatkov na najustreznejši center 112.

Glasovni klici in podatki MSD se usmerijo na najustreznejši center 112. Podatki MSD se v dekodirani obliki prenašajo na isti center prek podatkovnega vmesnika, v večini primerov z uporabo protokola SOAP. Poleg tega sistem eCall Node omogoča hkratni prenos podatkov MSD – skladno z regulativo in zakonodajo – tudi na druge naslovnike, torej do ostalih potencialnih deležnikov storitev eCall. Primer zanje so ponudniki storitev, povezanih s storitvijo eCall in njenimi podatki.

Rešitev eCall v Sloveniji je napredna, temelji na tehnologijah IP in je že pripravljena za nadgradnje v smeri naslednje generacije storitve eCall (NG eCall), ki jo bomo opisali v nadaljevanju. Podprli jo bomo po zaključeni standardizaciji.

C. *Minimalna zbirka podatkov (MSD)*

Minimalna zbirka podatkov, ki jih vozilo pošlje v klicni center v skladu z standardom SIST EN 17522:2011, vključuje:

– nadzorna polja:
  – samodejna/ročna aktivacija,
  – zaupanja vreden položaj,
  – vozilo (razredi):
– potnik M1,
– avtobusi M2, M3,
– lahka gospodarska vozila N1,
– težka vozila N2, N3,
– motorna kolesa L1e-L7e
– identifikacija (številka VIN),
– pogonsko gorivo (bencin, dizelsko gorivo, EV, LPG, CNG, vodik, …),
– časovna značka,
– lokacija, zadnje lokacije (n-1), (n-2) in smer vožnje (0-358),
– število potnikov (podatek pridobljen na podlagi števila varnostnih pasov).

VI. NADGRADNJE IN RAZŠIRITVE SISTEMA ECALL

A. *Storitev NG eCall*

Operaterji mobilnih omrežij prehajajo na tehnologijo LTE (Long Term Evolution), imenovano tudi mobilna tehnologija 4G. LTE omrežja so zgrajena na paketni komutaciji (Packet Switched – PS), kjer je normalen modus operandi oddaja paketov podatkov namesto namenskega komunikacijskega kanala, kar je značilnost tradicionalne vodovne komutacije (Circuit Switched – CS). Kot smo omenili, je storitev eCall trenutno standardizirana tako, da vzpostavlja govorni kanal in pošilja podatke v njem. LTE ne temelji na tehnologijah vodovne komutacije, zato klasična izvedba klica v sili za vozila ni mogoča. Nadomesti jo tehnologija paketne komutacije, ki temelji na tehnologiji IMS (IP Multimedia Subsystem – IMS), ki je arhitekturni okvir za zagotavljanje multimedijskih storitev v vseh omrežjih IP [9][10][12]. Veliko potrebnih funkcij za podporo sistemu eCall v okolju IP je že standardiziranih v okviru naslednje generacije sistema 112. MSD se prenaša izven govornih sporočil v signalizacijskih sporočilih, kar predstavlja tudi hitrejši prenos le-teh.

NG eCall omogoča celovitejši nabor podatkov (npr. regionalno specifični podatki, medicinski podatki potnikov, posebni podatki vozila), izboljšano funkcionalnost (npr. omogočanje osebju PSAPov, da si ogledajo video posnetke iz kamere na vozilu) in dvosmerna komunikacija, ki omogoča pošiljanje navodil vozilom (npr. zvok trobila, utripajoče luči, zaklepanje / odklepanje vrat, onemogočanje kontakta).

Storitev NG eCall bo še dodatno obogatila storitev eCall, ki bo poleg klasične uporabe v nujnih primerih omogočala tudi inovativne in uporabne storitve tretjih strank.

B. Storitev eCall za prevoz nevarnih snovi ter tovornjake in motoriste

Sedanji standard ne vsebuje ustreznih nastavkov za pridobivanje odločilnih informacij v primeru nenačrtovanih prometnih storitev, prevoza nevarnega blaga [15][16], in prevoza velikega števila ljudi. Prav tako ne podpira uporabe storitve eCall za dvokolesa oziroma motoriste.

C. Evropski projekt I_HeERO

V okviru kandidature pri projektu I_HeERO je Slovenija kot država pridobila status polnopravne članice s partnerji Upravo RS za zaščito in reševanje, Telekomom Slovenije d.d. in Iskratelom d.o.o. V okviru te akcije, ki je v fazi ocenjevanja pri Evropski komisiji, bodo vključene vse zgoraj navedene razširitve, in sicer podpora NG eCallu ter storitvi eCall za prevoz nevarnih snovi, tovornjake in motoriste. Prav tako bo poseben poudarek na izmenjavi podatkov.

VII. ZAKLJUČEK

Sčasoma bodo vsa vozila opremljena z napravami sistema eCall in tedaj pričakujemo znatni vpliv na zmanjšanje posledic prometnih nesreč. Infrastruktura eCall in podatki o prometnih nesrečah se skladno z zakonodajo in regulacijo lahko uporabljajo za zagotavljanje storitev tretjih oseb na področju preprečevanja goljufij, urejanja prometa, zagotavljanje varnosti prometa in prevoznih storitev, kot tudi prevoza nevarnega blaga. Z uvedbo NG eCalla na osnovi IP in paketne komutacije bodo dane dodatne možnosti in priložnost za razvoj storitev tretjih oseb. NG eCall bo omogočil bogatejši prenos podatkov in v povezavi z omrežji LTE tudi prenos videa.

Rešitev eCall, uvedena v Sloveniji, zagotavlja ustrezno podlago za ustvarjanje storitev tretjih strank že od samega začetka. Poleg tega je platforma pripravljena za prehod na NG eCall, ki bo uveden takoj, ko bo standardizacija zaključena. Tako bomo odprli pot za razvoj novih, inovativnih storitev, ki temeljijo na sistemu eCall.

ZAHVALE

Operacijo Usklajeni eCall je delno financirala Evropska unija iz Evropskega sklada za regionalni razvoj po pogodbi št. 3330-13-500310 z Ministrstvom za izobraževanje, znanost in šport.

LITERATURA

[1] Generalni direktorat za mobilnost in promet pri Evropski komisiji http://ec.europa.eu/dgs/transport/index_en.htm

[2] Road Transport, A change of gear, http://ec.europa.eu/transport/modes/road/doc/broch-road-transport_en.pdf

[3] BELA KNJIGA, Načrt za enotni evropski prometni prostor – na poti h konkurenčnemu in z viri gospodarnemu prometnemu sistemu, COM(2011) 144 konč. http://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:52011DC0144&from=EN

[4] Road safety in the European Union; Trends, statistics and main challenges, published by European Commission, Mobility and Transport DG, March 2015 http://ec.europa.eu/transport/road_safety/pdf/vademecum_2015.pdf

[5] Akcijski načrt CARS 2020, http://ec.europa.eu/enterprise/sectors/automotive/cars-2020/index_en.htm

[6] Poročilo CARS 2020, oktober 2014; http://ec.europa.eu/enterprise/sectors/automotive/cars-2020/index_en.htm#h2-1

[7] Boštjan Tavčar, *eCall – ne samo klic v sili*, Pametna mesta, Zbornik 28. delavnice o telekomunikacijah VITEL, Brdo pri Kranju, 12 .11. 2012, pp. 73—74.

[8] Projekt HeERO http://www.heero-pilot.eu/view/en/ecall.html (February 2015)

[9] Rainer Liebhart, Devaki Chandramouli, Curt Wong, Jurgen Merkel, LTE for Public Safety, Johm Wiley & Sons, ISBN: 978-1-118-82986-8

[10] European Automobile Manufacturers Association Position Pater on eCall, http://www.acea.be/publications/article/acea-position-ecall (february, 2015)

[11] ECDG "e-Call economic impact for society: contribution to rational analysis on benefits", September 2004

[12] eCall EENA Operations Document, Version 2.0, http://www.eena.org/uploads/gallery/files/pdf/2014_10_28_3_1_5_eCall_Update_v2.0_FINAL.pdf, August 2014

[13] European Transport Safety Council (ETSC): Position on eCall - New Pan-European Emergency Call System, http://archive.etsc.eu/documents/eCall_ETSC_Position_30%20September%202013.pdf, September 2013

[14] ROHS Directive; http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1399998664957&uri=CELEX:02011L0065-20140129

[15] Understanding REACH, ECHA-European Chemicals Agency; http://echa.europa.eu/web/guest/regulations/reach/understanding-reach

[16] European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR 2011); http://www.unece.org/trans/danger/publi/adr/adr2011/11ContentsE.htm

Ana Robnik je svetovalka za telekomunikacije. Koordinira delo v standardizacijskih organizacijah in vodi raziskovalno skupino podjetja Iskratel. Svojo poklicno pot je po univerzitetnem študiju uporabne matematike na Fakulteti za matematiko, fiziko in mehaniko in opravljenem magisteriju iz računalništva na Fakulteti za računalništvo nadaljevala v razvojno raziskovalni enoti Iskra Kibernetika. Nato se je vključila v razvoj telekomunikacijskih produktov SI2000 in SI3000 ter do leta 2009 vodila sektor za upravljanje in nadzor omrežnih elementov portfelja podjetja Iskratel.

Gorazd Novak je diplomiral na Fakulteti za elektrotehniko in zaključil magistrski študij na Ekonomski fakulteti. Leta 1989 se je zaposlil v podjetju Iskratel, kjer je opravljal različne upravljavske funkcije. Osredotočil se je na oblikovanje komunikacijskih omrežij in rešitev. Trenutno je upravljavec rešitev (Solution Manager) javne varnosti v izjemnih razmerah.

Komunikacije kot kritična infrastruktura na področju varstva pred naravnimi in drugimi nesrečami

Marko Podberšič, MORS, Uprava Republike Slovenije za zaščito in reševanje

Povzetek — V članku so opisane različne vrste komunikacijskih sistemov, ki se uporabljajo na področju varstva pred naravnimi in drugimi nesrečami ter izkušnje z njihovo uporabo ob večjih naravnih in drugih nesrečah. Na koncu so podani predlogi za njihov nadaljnji razvoj in izboljšanje.

Ključne besede — kritična infrstruktura, radijski komunikacijski sistemi, ZARE

Abstract — This article describes the different types of communication systems used in the field of protection against natural and other disasters, and how to use them in major natural and other disasters. Finally, suggestions are given for their further development and improvement.

Keywords — critical infrastructure, radio communication systems, ZARE

I. UVOD

Ob večjih naravnih in drugih nesrečah, še posebno ob tako obsežnih, kot je bila ujma z žledom, ki je februarja 2014 zajela skoraj celo državo, opažamo, kako pomembno je zanesljivo delovanje vseh komunikacijskih sistemov v takšnih razmerah. To zagotovo velja za komunikacijske sisteme služb za zaščito reševanje in pomoč.

Ti komunikacijski sistemi nedvomno spadajo med kritično infrastrukturo in je zanje potrebno vzpostaviti visok nivo avtonomije delovanja tudi ob izpadu omrežnega napajanja ali izpadu drugih komunikacijskih povezav. Okvara oz. nedelovanje teh komunikacijskih sistemov lahko vpliva na zdravje in varnost ljudi, živali in premoženja.

II. KRITIČNA INFRASTRUKTURA

Pojem kritična infrastruktura zajema predvsem:

- energetske sisteme (elektrika, nafta, plin),
- komunikacijske in informacijske sisteme,
- transportne sisteme (cestne, železniške, zračne, pomorske),
- finančne sisteme,
- sisteme zdravstvene oskrbe,
- sisteme za preskrbo s hrano,
- sisteme za preskrbo s pitno vodo,
- varovanje zdravega okolja.

Pod kritično infrastrukturo nekateri avtorji prištevajo tudi državne inštitucije, različne reševalne službe in nekatere pomembnejše industrijske panoge.

Pojmovanje kritične infrastrukture se je s časom spreminjalo. Včasih so med kritično infrastrukturo uvrščali predvsem tisto infrastrukturo, katere daljše motnje bi lahko povzročile večje vojaške ali ekonomske posledice. Danes je kritična infrastruktura izjemno široka kategorija. Njena razširitev je tudi posledica vzpona terorizma, kot globalno pomembne grožnje varnosti [1].

V članku sem se osredotočil na zasebne komunikacijske sisteme, ki jih uporabljajo različne službe za zaščito reševanje in pomoč. Ti sistemi so nedvomno del kritične infrastrukture.

III. ZASEBNI KOMUNIKACIJSKI SISTEMI SLUŽB ZA ZAŠČITO REŠEVANJE IN POMOČ

Službe za zaščito, reševanje in pomoč v Sloveniji uporabljajo različne zasebne profesionalne komunikacijske sisteme. Predvsem sistemi radijskih komunikacij na tem področju so praviloma zasebni, saj morajo biti posebej prilagojeni za delo ob večjih naravnih in drugih nesrečah.

A. Sistem radijskih zvez ZARE

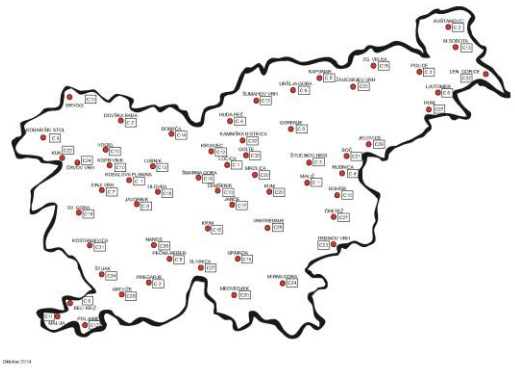
Predhodnik obstoječega sistema radijskih zvez ZARE, je bilo omrežje gasilskih repetitorskih postaj. To je v obdobju pred letom 1994 uspešno služilo svojemu namenu. Z novo organizacijo sistema varstva pred naravnimi in drugimi nesrečami, zlasti z ustanovitvijo centrov za obveščanje, je bilo nujno na novo organizirati tudi sistem radijskih zvez.

Vzpostavljen je bil enoten sistem, ki je organiziran tako, da ima vsaka regija svoj avtonomen del sicer enotnega sistema. S sistemom po posameznih regijah upravljajo pristojni regijski centri za obveščanje. Radijska zveza med dvema reševalcema, ki se nahajata v različnih regijah, praviloma ni mogoča [2].

Sistem radijskih zvez ZARE je klasični analogni sistem, zgrajen na frekvenčnih področjih VHF in UHF na način, da repetitorske radijske postaje delujejo na frekvenčnem področju VHF, njihove neposredne povezave v pristojne regijske centre za obveščanje pa na frekvenčnem področju UHF.

Takšen koncept daje prednost dostopa do repetitorske radijske postaje operaterju v regijskem centru za obveščanje. Opisani sistem radijskih zvez je namenjen za govorne komunikacije, ni pa primeren za prenos podatkov.

Po obsegu je sistem radijskih zvez ZARE največji enotni profesionalni sistem radijskih zvez v državi. Sestavljen je iz 63 repetitorskih postaj in zagotavlja 95 % pokritost terena z radijskih signalom. Postavitev repetitorskih postaj sistema zvez ZARE prikazuje slika 1. Na mestih, kjer je pokritost z radijskim signalom slabša, je predvidena uporaba mobilnih repetitorjev.



Slika 1: Repetitorji sistema radijskih zvez ZARE

B. Sistem osebnega klica - paging

Tudi začetki sistema osebnega klica segajo v leto 1994, ko se je začel graditi sistem radijskih zvez ZARE. Sistem osebnega klica je bil do prenove del sistema radijskih zvez ZARE, saj je za komunikacijo med računalniki za proženje pozivnikov v centrih za obveščanje in oddajniki na višinskih točkah uporabljal iste povezave UHF.

Tako kot sistem zvez ZARE, je tudi sitem osebnega klica organiziran tako, da ima vsaka regija svoj avtonomen del sicer enotnega sistema. Organizacija dela centrov za obveščanje je takšna, da posamezni regijski centri za obveščanje prožijo le sprejemnike osebnega klica na svojem območju, Center za obveščanje Republike Slovenije pa lahko proži vse pozivnike v državi.

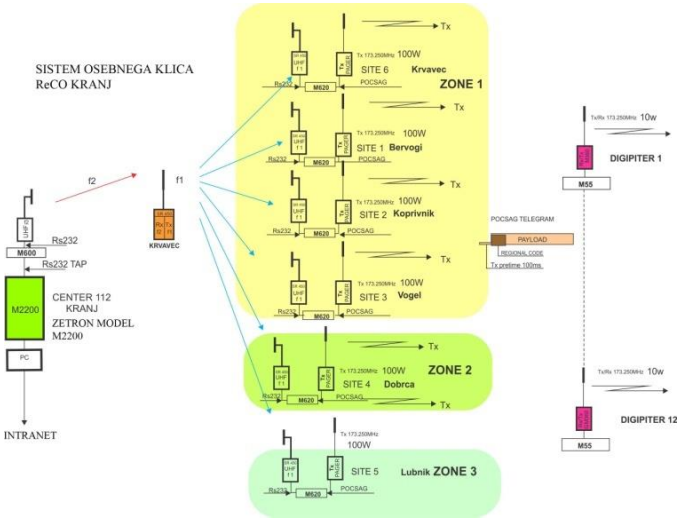
Sistem deluje po standardu POCSAG in omogoča pošiljanje sporočil dolžine do 155 znakov posameznikom ali skupinam. Deluje v frekvenčnem področju VHF na frekvenci 173,250 MHz, uporablja kanal širine 12,5 kHz.

Sistem osebnega klica je bil v letih 2010 do 2012 v celoti prenovljen in ločen od sistema zvez ZARE. Dodane so bile prenosne radijske poti UHF, ki služijo za povezavo opreme v regijskih centrih za obveščanje z oddajniki na višinskih točkah. Prav tako je bilo prenovljeno rezervno napajanje na višinskih točkah.

Računalniki za proženje pozivnikov so med seboj povezani prek lokalnega računalniškega omrežja ZIR, kar omogoča, da proženje sprejemnikov osebnega klica na območju enega regijskega centra za obveščanje lahko prevzame drug center za obveščanje. Prav tako prenovljeni sistem osebnega klica omogoča oddaljena dispečerska mesta, ki so nujno potrebna za nekatere strukture reševalcev.

Zgradbo sistema osebnega klica v gorenjski regiji prikazuje slika 2. Kontrolni strežnik Zetron M2200 sporočila osebnega klica posreduje oddajniku prek modula Zetron M600, UHF radijske povezave in modula Zetron M620, ki se nahaja neposredno ob oddajniku. Modul Zetron M620 skrbi za kodiranje sporočila POCSAG in krmili oddajnik. Ta odda sporočilo osebnega klica z uporabo modulacije DFSK s hitrostjo 1200 bit/sek.

V sistemu osebnega klica se uporablja sekvenčno oddajanje sporočila prek več oddajnikov. Oddajniki so združeni v skupine (ZONE 1, ZONE 2, ZONE 3). Oddajniki v isti skupini gredo na oddajo istočasno. Z uporabo sekvenčnega oddajanja se izognemo motnjam na območjih prekrivanja radijskega signala. Za pravilno sekvenčno oddajanje skrbi kontrolni strežnik Zetron M2200.



Slika 2: Zgradba sistema osebnega klica v gorenjski regiji

V Centru za obveščanje Republike Slovenije je nameščen kontrolni strežnik Zetron M2200, ki vsebuje podatke o vseh sprejemnikih osebnega klica v državi. V vsakem regijskem centru za obveščanje pa je nameščen kontrolni strežnik Zetron M2200 s podatki o sprejemnikih osebnega klica v določeni regiji.

Sistem osebnega klica je povezljiv s sistemom PLK (prikaz lokacije kličočega), tako da je mogoče iz sistema PLK neposredno pošiljati pozive na sprejemnike osebnega klica. Za povezavo obeh sistemov je uporabljen protokol TAP [3].

Nov sistem osebnega klica je mogoče upravljati tudi z oddaljene lokacije prek protokola IP. Zunanje upravljanje sistema je mogoče prek oddaljene nadzorne postaje z namensko aplikacijo.

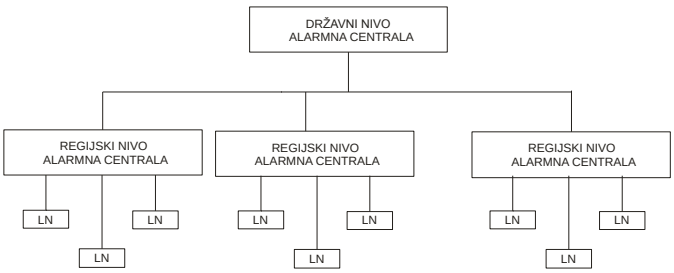
Oddaljena nadzorna postaja je prek VPN povezave povezana v omrežje naprav za proženje sprejemnikov osebnega klica. Tako omogočamo nekaterim reševalnim službam, da lahko same prožijo svoje sprejemnike osebnega klica. Uprava RS za zaščito in reševanje nudi le vstopno točko v omrežju internet, strošek razvoja namenske aplikacije in vzpostavitve VPN povezave odpade na posamezno reševalno službo, ki želi omenjeno storitev vzpostaviti.

C. Sistem javnega alarmiranja (SIJA)

Sistem javnega alarmiranja v Republiki Sloveniji je v fazi prenove. Ministrstvo za obrambo, Uprava Republike Slovenije za zaščito in reševanje, bi morala na osnovi novele Zakona o varstvu pred naravnimi in drugimi nesrečami do leta 2011 postopoma prenoviti in prevzeti sistem javnega alarmiranja na lokalnem nivoju. Izvzete so le alarmne naprave, za katere so dolžne skrbeti gospodarske družbe, zavodi in druge organizacije. Zaradi nastale finančne in gospodarske krize prenova in prevzem še nista zaključena. Do sedaj smo prenovili slabih 60% siren.

Zasnova sistema javnega alarmiranja v Republiki Sloveniji je hierarhična in obsega tri nivoje (slika 3):

- državni,
- regijski,
- lokalni.



Slika 3: Zgradba sistema javnega alarmiranja

Sistem javnega alarmiranja je sestavljen iz naslednjih podsistemov:

- alarmna centrala z ustrezno programsko opremo,
- lokalno računalniško omrežje ZIR,
- radijska vstopna točka v regijskih centrih za obveščanje,
- zasebni digitalni sistem radijskih zvez,
- elektronska sirena in
- mobilni sistem javnega alarmiranja.

i. Alarmna centrala

Alarmne centrale so računalniki, s katerih prožimo sirene. Alarmne centrale so nameščene v vseh centrih za obveščanje. Med seboj so povezane prek računalniškega omrežja ZIR.

Programska oprema je namenska in služi za daljinsko krmiljenje elektronskih siren ter za nadzor nad njimi. Zasnovana je tako, da lahko vsak regijski center za obveščanje prevzame vlogo drugega. Pogoj je, da je alarmna centrala povezana v lokalno računalniško omrežje ZIR.

ii. Računalniško omrežje ZIR

Lokalno računalniško omrežje ZIR je računalniško omrežje, s katerim upravlja Uprava RS za zaščito in reševanje. V sistemu javnega alarmiranja služi za povezavo alarmnih central.

iii. Radijska vstopna točka

Radijska vstopna točka je nameščena v vsakem regijskem centru za obveščanje. Radijska vstopna točka je radijska naprava DMR, ki je povezana v lokalno računalniško omrežje ZIR. Služi kot vmesnik med alarmno centralo in sirenami, ki so z radijsko vstopno točko povezane prek zasebnega digitalnega sistema radijskih zvez ZARE DMR.

iv. Zasebni digitalni sistem radijskih zvez ZARE DMR

Radijsko omrežje ZARE DMR deluje v področju VHF in sicer v istem frekvenčnem spektru kot sistem analognih govornih zvez ZARE, le da je frekvenčni korak med oddajno in sprejemno frekvenco 4,6 MHz (pri sistemu govornih zvez je 4,5 MHz). Poleg tega pa radijsko omrežje deluje v digitalnem režimu po protokolu ETSI 102-361÷363. Omrežje postopoma gradimo od leta 2006, trenutno je sestavljeno iz 37 repetitorjev DMR.

Daljinsko krmiljenje in nadzor nad sistemom javnega alarmiranja deluje prek sistema ZARE DMR. To je tudi primarna naloga tega radijskega sistema, poskusno pa se uporablja tudi za prenos govora.

Prednosti tehnologije DMR pred analogno tehnologijo:

- Tehnologija DMR temelji na časovnem sodostopu (TDMA), kar ji omogoča dva logična kanala znotraj fizičnega kanala širine 12.5 kHz. To pomeni podvojitev zmogljivosti sistema in znižanje stroškov.
- Posebna tehnologija odprave napak omogoča boljšo kvaliteto zvoka.
- Radijski sistemi DMR lahko delajo v analognem ali digitalnem načinu.

v. Elektronska sirena

Elektronska sirena je v sistemu javnega alarmiranja sestavljena iz:

- elektronske sirene same,
- napajalnega sistema in
- VHF radijske postaje s podatkovnim vmesnikom.

Elektronska sirena je naprava, ki prek NF-ojačevalnikov in zvočnikov proizvaja zvočne alarme in govorna sporočila. Alarmne znake je mogoče aktivirati lokalno na napravi sami, ali daljinsko iz centra za obveščanje.

V sistemu javnega alarmiranja so uporabljene elektronske sirene moči od 250W do 1000W z različnimi koti postavitve zvočnikov.

vi. Mobilni sistem javnega alarmiranja

Namen mobilnega sistema javnega alarmiranja je interventna postavitev sistema javnega alarmiranja na področjih na katerih je prebivalstvo zelo ogroženo zaradi ujm (npr. plaz, povodenj itd.). Mobilni sistem javnega alarmiranja omogoča hitro začasno postavitev. Sestavi deli mobilnega sistema so:

- avtomatska opazovalnica,
- mobilna elektronska sirena in
- semafor.

IV. IZKUŠNJE OB NARAVNIH IN DRUGIH NESREČAH

Izkušnje z uporabo opisanih zasebnih komunikacijskih sistemov služb za zaščito, reševanje in pomoč v primeru naravnih in drugih nesreč so v splošnem dobre. Če se nesreča zgodi na območju, ki je slabše pokrito z radijskim signalom sistema radijskih zvez ZARE, se uporabi mobilni repetitor.

Uprava RS za zaščito in reševanje (URSZR) je v lanskem letu kupila 13 novih mobilnih repetitorjev, za vsako izpostavo URSZR po enega. Gasilska zveza Slovenije je določila 13 ekip, ki jih usposabljamo za uporabo in postavitev teh mobilnih repetitorjev. Te ekipe bobo, ko bodo usposobljene, mobilni repetitor lahko postavile kjerkoli v Republiki Sloveniji ali tujini.

Ujma z žledom, ki je februarja leta 2014 prizadela skoraj celotno Slovenijo, je pokazala tudi na ranljivost komunikacijskih sistemov, ki jih uporabljajo sile za zaščito, reševanje in pomoč. Okvare na električnih daljnovodih in omrežjih ter otežen ali onemogočen dostop do TK objektov na višinskih točkah so bili glavni vzroki izpada nekaterih repetitorjev sistemov radijskih zvez ZARE in ZARE DMR ter oddajnikov sistema osebnega klica. Dodaten vzrok za izpade omenjenih sistemov je bil leden oklep, ki se je nabral okrog anten na antenskih stolpih. Ob taljenju in odpadanju ledenega oklepa, so padajoči kosi ledu poškodovali nižje ležeče antene.

Sistema radijskih zvez ZARE, ZARE DMR in sistem osebnega klica imajo lastno akumulatorsko rezervno napajanje, ki zagotavlja 7 dni avtonomije ob izpadu omrežnega napajanja, pri načinu delovanja 50/50. Avtonomija pri sistemu osebnega klica je dejansko še nekoliko večja.

Akumulatorsko napajanje siren sistema javnega alarmiranja omogoča njihovo delovanje še 6 dni po izpadu omrežnega napajanja ob predpostavki 20 proženj posamezne sirene z alarmnimi znaki dolžine 1 minute.

Zaradi varčevalne politike v letih 2012 in 2013 so bili, ob ujmi z žledom, akumulatorji v sistemu zvez ZARE stari in potrebni menjave. Zato so, na tistih lokacijah, kjer je prišlo do izpada električne energije, najprej ugasnili repetitorji sistema zvez ZARE, nato pa še ostali sistemi.

Izpad posameznih repetitorjev ZARE smo hitro nadomestili z mobilnimi repetitorji, ki so jih v okolici izpadlih repetitorjev postavili predstavniki enote za zveze civilne zaščite in delavci URSZR. Tam, kjer je bilo to potrebno, smo mobilne repetitorje napajali z agregati in organizirali preskrbo z gorivom.

Na vseh telekomunikacijskih objektih v upravljanju Ministrstva za obrambo, smo zagotovili napajanje s pomočjo električnih agregatov, na katere smo priključili tudi opremo javnih telekomunikacijskih operaterjev. Pri vzpostavljanju ponovnega delovanja naših radijskih sistemov so nam izdatno pomagali serviserji javnih telekomunikacijskih operaterjev, med njimi tudi Telekoma Slovenije.

V. NADALJNJI RAZVOJ RADIJSKIH SISTEMOV

Sistem osebnega klica je popolnoma samostojen in neodvisen radijski sistem in je bil prenovljen v letih od 2010 do 2012. V prihodnjih letih pričakujemo porast oddaljenih nadzornih postaj, ki bodo posameznim reševalnim službam omogočale, da same prožijo svoje sprejemnike osebnega klica.

Nadaljevali bomo s prevzemom sistema javnega alarmiranja na lokalnem nivoju, tudi s pomočjo različnih evropskih projektov. Krmiljenje in nadzor sistema bo še naprej potekalo prek radijskega omrežja DMR.

Oprema sistema radijskih zvez ZARE je v povprečju stara petnajst let. Sistem je sicer v dobrem tehničnem stanju, vendar potreben prenove in posodobitve. Nadomestilo ga bo enotno digitalno radijsko omrežje državnih organov.

Sklep vlade RS, št. 007/148/2009/, z dne 26. 11. 2012, predvideva vzpostavitev enotnega digitalnega radijskega omrežja državnih organov Republike Slovenije v obliki hibridne (kombinirane) rešitve z uporabo dveh standardiziranih digitalnih tehnologij v dveh fazah:

- V prvi fazi se dokonča digitalno radijsko omrežje Policije v obsegu, kot ga predvideva tehnična dokumentacija. Prav tako se v prvi fazi zagotovi povezava med obstoječim radijskim omrežjem zaščite in reševanja ter digitalnim radijskim omrežjem Policije v izgradnji. Nosilec je Ministrstvo za notranje zadeve.
- V drugi fazi se v skladu z iztekajočo dobo uporabnosti naprav obstoječega radijskega sistema postopoma digitalizira radijsko omrežje zaščite in reševanja ter optimizira enotno digitalno radijsko omrežje. Nosilec je Ministrstvo za obrambo.

Predlagana rešitev predstavlja optimizacijo tehničnih možnosti, ki jih ponuja digitalna tehnologija na področju radijskih povezav in vzpostavitev medsebojnih radijskih komunikacij različnih uporabniških skupin. Upoštevan je postopen prehod uporabnikov v novo digitalno radijsko omrežje, s čimer bo zagotovljena tudi optimizacija stroškov v prehodnem obdobju.

Sklep vlade torej predvideva, da se enotno digitalno radijsko omrežje državnih organov Republike Slovenije vzpostavi s kombinacijo standardiziranih tehnologij TETRA (digitalno radijsko omrežje Policije) in DMR (digitalno radijsko omrežje zaščite in reševanja).

Območje pokrivanja repetitorske postaje DMR je večje kot pokrivanje bazne postaje TETRA. Teoretično največji doseg baznih postaj TETRA je 58 km. Pri večji razdalji izpade sinhronizacija logičnih kanalov. Priporočljiva minimalna jakost signala za sisteme TETRA je -90 dBm. Teoretični doseg repetitorske postaje DMR je 150 km. Zaradi večje občitljivosti radijskih postaj DMR je priporočljiva minimalna jakost signala -100 dBm. Območje pokrivanja repetitorskih postaj DMR je zato večje, kot pri baznih postajah TETRA [4].

Organizacija dela posameznih reševalnih služb je takšna, da na mestu intervencije, komunikacija med udeleženci intervencije poteka v neposrednem načinu dela, brez posredovanja repetitorja oz. bazne postaje. Tudi tu ima komunikacija med radijskimi postajami DMR, zaradi praviloma večje moči oddajnika in boljše občutljivosti sprejemnika, daljši domet, kot komunikacija med radijskimi postajami TETRA.

VI. ZAKLJUČEK

Na področju zaščite in reševanja uporabljamo različne zasebne radijske komunikacije sisteme. Izkušnje z njihovo uporabo ob večjih naravnih in drugih nesrečah so v splošnem dobre.

Ujma z žledom, ki je februarja leta 2014 prizadela skoraj celotno Slovenijo, je povzročila tudi izpade posameznih delov teh radijskih komunikacijskih sistemov, predvsem zaradi izpadov omrežnega napajanja. Izpade smo hitro nadomestili s postavitvijo mobilnih repetitorjev oz. zagotavljanjem električnega napajanja s pomočjo agregatov. Vlada Republike Slovenije je v svojem sklepu ugotovila, da je bilo aktiviranje in delovanje sil za zaščito reševanje in pomoč pravočasno in ustrezno.

LITERATURA

[1] Miha Žnidar, Diplomsko delo, Vpliv lastništva kritične infrastrukture na nacionalno varnost Republike Slovenije, Univerza v Ljubljani, Fakulteta družbene vede, 2009

[2] http://www.sos112.si/slo/page.php?src=pr12.htm

[3] FERI, IJS, IGEA, CRP razvojno raziskovalni projekt: Izdelava koncepta razvoja IT in strategija zbiranja, vzdrževanja in vodenja podatkov, Maribor, Ljubljana, 2008

[4] Boštjan Tavčar, Radijske komunikacije v mednarodnih reševalnih operacijah.

Dr. **Marko Podberšič** je diplomiral na Fakulteti za elektrotehniko, računalništvo in informatiko v Ljubljani, magistriral in doktoriral pa na Fakulteti za elektrotehniko, računalništvo in informatiko v Mariboru. V letih 1989 – 2002 je bil zaposlen v razvojnem oddelku podjetja Iskraemeco, d.d. Od leta 2002 je zaposlen na Ministrstvu za obrambo, Upravi RS za zaščito in reševanje. Opravlja tudi delo višješolskega pradavatelja na Višji strokovni šoli za telekomunikacije, Šolskega centra za pošto, ekonomijo in telekomunikacije.

Digitalizacija sistema zvez ZARE

Jože Štuflek, IT 100, d.o.o., Brezovica pri Ljubljani

Povzetek — Iztekajoča se uporaba analognega sistema radijskih zvez ZARE narekuje postopno digitalizacijo tega sistema po tehnologiji DMR (digitalni mobilni radijski sistem), zato je potrebno poiskati najustreznejšo tehnično rešitev, pri tem pa opredeliti tudi ustreznost finančne obremenitve prehoda na digitalizacijo. Predlog nadgradnje oziroma digitalizacije upošteva vse možne tehnične rešitve, predvsem v smislu, da se uporabi že nabavljena radijska oprema na terenu. Posebno pozornost je potrebno nameniti načinu delovanja in načinu praktične uporabe uporabnika. Predstavljena bo ena od možnih tehničnih rešitev - Link Capacity Plus. Ta rešitev je po našem mnenju najustreznejša, še posebno, če upoštevamo opremo DMR na terenu (več kot 5000 radijskih naprav Mototrbo) in podobnost z obstoječim analognim sistemom radijskih zvez ZARE, nenazadnje pa tudi iz praktičnih izkušenj v že postavljenem in delujočem radijskem sistemu DMR v naši državi, ki prav tako deluje v tehnologiji Link Capacity Plus.

Ključne besede — digitalizacija, sistem radijskih zvez ZARE, snopovni sistem, Link Capacity Plus

Abstract — Escaping the use of an analog radio system ZARE requires a gradual digitalization of the system by technology DMR (digital mobile radio system), it is necessary to find the most appropriate technical solution, while also define the adequacy of the financial budget of the transition to digitalization. The proposal upgrades and digitalization takes into account all possible technical solutions, especially in the sense that it is used already purchased radio equipment in the field. Special attention should be given to mode and manner of the practical application of the beneficiary. Presented will be one of the possible technical solutions - Link Capacity Plus. This solution is in our opinion the most appropriate, especially when considering the DMR equipment on the ground (more than 5000 radio devices Mototrbo) and similarity with the existing analogue radio communications system ZARE, last but not least, also from practical experience in a direct and active DMR radio system in our country, which also operates in the technology of Link Capacity Plus.

Keywords — digitization, the system of radio communications ZARE, trunking system, Link Capacity Plus

I. UVOD

Sistem radijskih zvez ZARE (sistem radijskih zvez Zaščita-Reševanje Ministrstva za obrambo, Uprave za zaščito in reševanje) je namenjen za radijsko komuniciranje vsem enotam strukture zaščite in reševanja. Izgradnja sistema se je začela v letih 1991-1992 in sicer na osnovi takratne radijske opreme, ki so jo imele enote civilne zaščite (CZ), posebej enote gasilcev in sicer poklicnih in profesionalnih gasilcev.
Z organizacijo regijskih centrov za obveščanje je bila tudi organizacija sistema zvez vezana na regijski model. Tako je bilo postavljenih 13 (trinajst) radijskih sistemov za 13 (trinajst) regij na področju R Slovenije kot je prikazano v nadaljevanju.

V vsaki regiji je ustrezno število repetitorjev na VHF obsegu, njihovo število je v posamezni regiji naraščalo skladno s potrebami in možnostmi. Smatra se, da je to število repetitorjev sedaj dokončno.

Tehnično je radijski sistem zasnovan tako, da se radijske postaje uporabljajo v semidupleksnem in simpleksnem načinu delovanja v 12,5 kHz širokem kanalu na frekvenčnem območju VHF in sicer na frekvenčnem pasu, ki je dodeljen za državno uporabo za sistem ZARE (Ur. List št. 17/2006).

Tabela 1: Regije in število repetitorjev po regijah

Zap.št.	Regija ReCO 112	Št. repetitorjev
1.	Celje	7
2.	Slovenj gradec	3
3.	Nova gorica	8
4.	Brežice	2
5.	Koper	3
6.	Kranj	7
7.	Ljubljana	7
8.	Maribor	4
9.	Murska Sobota	5
10.	Novo mesto	3
11.	Postojna	7
12.	Ptuj	2
13.	Trbovlje	3
Skupaj:		**61**

Tabela 2: Dodeljene frekvence iz Načrta uporabe radijskih frekvenc za državno uporabo (ZARE)

VHF	UHF
168,550	404,900
↓	↓
169,075	405,000
173,050	409,900
↓	↓
173,575	410,000

Pri tem pa v takratni dodelitvi posamezne frekvence za repetitorsko VHF-napravo ni bilo upoštevano priporočilo TR-25, tako, da frekvenčni niz ni bil v celoti izkoriščen. Ta pomanjkljivost je bila kasneje odpravljena in sicer za realizacijo sistema javnega alarmiranja.

Za pokrivanje področij, kjer je pokritost osnovnega sistema slabša, se uporabljajo tudi mobilni repetitorji, za katere sta določena 2 (dva) frekvenčna para.

Vse to je namenjeno za govorne zveze.

Regijski centri so opremljeni s komunikacijskimi konzolami, katere so neposredno povezane z vsako bazno – repetitorsko postajo na svojem področju in sicer preko radio

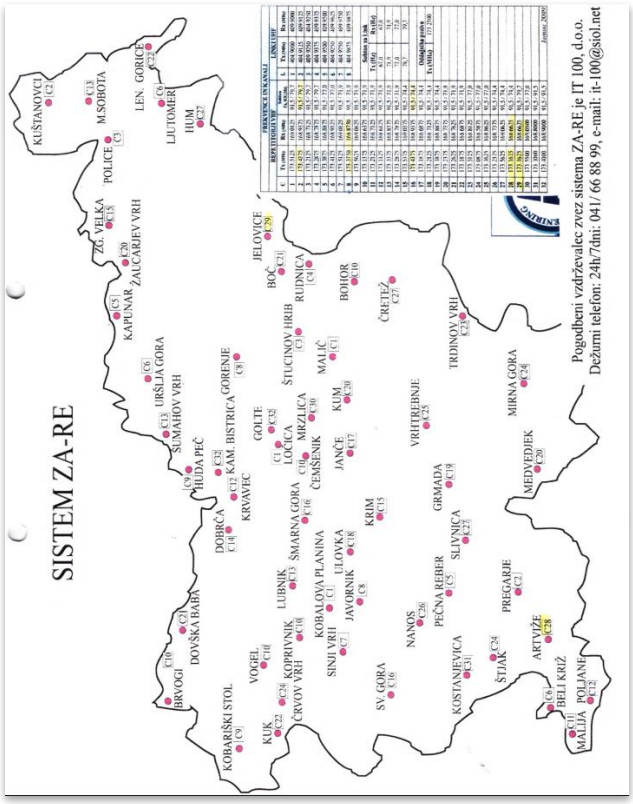
mosta (usmerjene zveze) – v frekvenčnem območju UHF v dupleksnem režimu dela. Preko teh konzol so mogoče vse vrste komutacije, kar pomeni podaljševanje radijskih zvez v telefonske in obratno ter radijske zveze med seboj.

Poleg sistema radijskih zvez za govorne zveze sta tukaj še dva sistema brezžičnih zvez: sistem enosmernega pozivanja – tiho alarmiranje SITA in sistem javnega alarmiranja – proženje javnih siren SIJA, preko neodvisne radijske mreže. Oba sistema sta v temeljiti prenovi z uporabo sodobne tehnologije v radijskih zvezah in sicer DMR – Digital Mobile Radio. Gre za digitalne prenose preko obstoječih frekvenčnih kanalov.

Podobna prenova na digitalne sisteme je potrebna tudi za govorne sisteme radijskih zvez. Potrebe na terenu narekujejo nove načine komunikacij in prav gotovo lahko te izzive rešujemo z novimi tehnologijami in ena od teh je odprt protokol za tovrstne radijske zveze ETSI 102-361 do 364.

Vsekakor pa mora prenova temeljiti na integraciji obstoječih sistemov in na podobnem, če že ne na enakem načinu delovanja, gledano s strani uporabnikov. Pomembno je, da se dosežejo zanesljivost delovanja.

Na sliki 1 je razviden trenutni razpored radijskih kanalov in lokacij baznih radijskih postaj sistema ZARE v analognem načinu delovanja.



Slika 1: Razpored radijskih kanalov in lokacije v sistemu ZARE

II. DIGITALIZACIJA SISTEMA

S pojavom novih tehnologij kot sta DMR in dpMR so tudi na tem področju nastale tehnične možnosti preureditve sistemov radijskih zvez ZARE in sicer po tehnično in ekonomsko sprejemljivih kriterijih.

Frekvenčni prostor, ki je namenjen tem uporabnikom, je omejen in ga je potrebno uporabiti tako, da bomo v tem prostoru zagotovili vse zahteve, ki jih od takšnih sistemov pričakujemo. Enostavno povedano je frekvenčni prostor naravna dobrina, s katero je potrebno ravnati gospodarno.

Namen integracije obstoječih sistemov, ki delujejo po dosedanjih analognih tehnologijah, je nadgradnja z novimi tehnologijami, pri tem pa se mora upoštevati vse kriterije medsebojne povezljivosti, stanje infrastrukture in tehnično-ekonomske učinke.

Širše gledano so v sistemu radijskih zvez ZARE osnovne zahteve naslednje:

- Pogovorne radijske zveze na nivoju regije s centrom za obveščanje – semidupleksen način dela;
- Simpleksne zveze za kratke medsebojne povezave na mikrolokaciji;
- Semidupleksne zveze na geografsko omejenem področju v primeru širše potrebe, ko simpleksne zveze ne pokrivajo področja, v tem primeru pride v poštev mobilni repetitor;
- Prenos enosmernih sporočil pozivov–tiho alarmiranje - enovito za vso državo;
- Dvosmerne telemetrijske radijske zveze za sistem SIJA;
- Dvosmerne telemetrijske radijske zveze za sistem sledenja.

Vse te zahteve morajo biti zagotovljene v dodeljenem frekvenčnem prostoru, skladno z vsemi nacionalnimi in internacionalnimi predpisi.

Dodeljene so frekvence iz področja VHF, ki jih je potrebno planirati in razširiti tako, da dobimo zadovoljivo število frekvenčnih parov za vse zahteve.

Pri prvih začetkih postavljanja sistema radijskih zvez ZARE ni bilo še dodeljenega frekvenčnega pasu v področju VHF, pač pa so bili dodeljeni posamezni diskretni frekvenčni pari. Zaradi tega ni bilo mogoče že na začetku narediti ustreznega frekvenčnega plana za vso državo. Sedaj je seveda potrebno upoštevati zatečeno stanje, pri tem pa je bistveno, da je dupleksni razmik 4,5 MHz, kar ni skladno s TR-25 (evropski tehnični predpis). Razmik mora biti 4,6 MHz in to tako, da je oddajna frekvenca bazne postaje v paru višja.

Pri prenovi in integraciji je to tudi novo izhodišče za frekvenčni plan.

Pri planiranju digitalnega radijskega sistema zvez je torej osnovno izhodišče obstoječe stanje, kar pomeni frekvenčno področje in terminalska oprema na terenu. Digitalne terminalske radijske naprave (mobilne, ročne) delujejo skladno z ETSI standardom TR-102, 361-362-363-364 in sicer TIR 2 DMR. Digital Mobile Radio (DMR) predvideva izvedbo naprav po TIR1, TIR2 in TIR3.

Kot je bilo predhodno omenjeno, digitalne radijske naprave, ki so v uporabi v sistemu Uprave RS za zaščito in reševanje ZARE, delujejo po DMR – TIR2. To je, seveda, izhodišče za izbiro vrste snopovnega sistema pri nadgradnji - digitalizaciji.

Nadgrajen – digitaliziran sistem mora zagotavljati poleg osnovnih zahtev v radijskem obstoječem analognem načinu delovanja predvsem večjo prometno prepustnost, enostavno uporabo terminalov, bolje pokrita ruralna področja, ki sedaj niso, povezljivost baznih postaj po internet protokolu IPv4.

Sistem naj bo tudi v digitalni snopovni obliki projektiran kot sistem, sestavljen iz trinajstih (13) regij, ki jih pokriva posamezen regijski center za obveščanje ReCO 112.

Pri planiranju sistema je potrebna posebna pozornost na naslednjih elementih:

- namen radijskih zvez,
- frekvenčno področje (v tem primeru VHF),

- razpoložljivost sistema (ang. Grade of Service),
- delovanje ob izrednih razmerah,
- rezervno napajanje,
- nadzor in upravljanje,
- povezljivost z »ostalimi sistemi«,
- šifriranje,
- možnost nadgradnje,
- prenos podatkov.

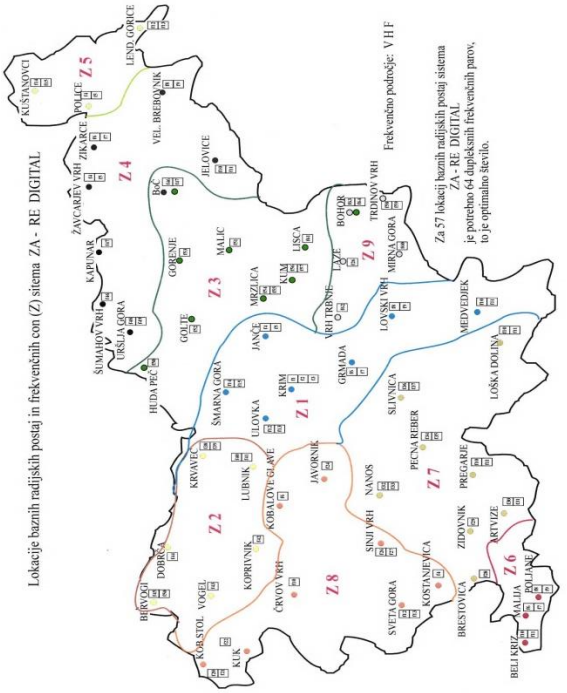
Pri analizi možnosti nadgradnje sistema radijskih zvez ZARE v sodoben digitalni snopovni sistem, ki mora zagotavljati vse zadane naloge in upoštevati več kot 5.000 radijskih terminalov, smo iskali tehnične in finančne možnosti nadgradnje tako, da se uporabi vsa obstoječa oprema, ki deluje po protokolu DMR in da pri tem ostanejo delujoče vse digitalne terminalske naprave tudi v dosedanjih režimih dela.

Pri izbiri snopovnega delovanja sistema smo bili posebej pozorni na konstantno porabo energije. Na tej podlagi smo dajali prednost sistemom, ki za snopovno delovanje ne potrebujejo neprekinjenega delovanja kontrolnega kanala pri baznih radijskih postajah, pri terminalski opremi pa tozadevno ne sme biti potrebna nobena strojna nadgradnja. Zaželeno je tudi, da v kolikor je potrebna programska nadgradnja, le-ta naj ne bo plačljiva.

Na osnovi vsega naštetega predlagamo nadgradnjo – digitalizacijo sistema radijskih zvez v snopovni (trunking) sistem po protokolu **Link Capacity Plus**. Snopovni sistem po tem protokolu omogoča petnajst (15) baznih radijskih postaj, med seboj povezanih po protokolu IP. Na vsaki lokaciji bazne radijske postaje je lahko osem (8) repetitorjev, t.j. osem (8) frekvenčnih nosilcev, pri čemer ima vsak dvoje časovnih oken. To velja za prenos govornih informacij, kar predstavlja šestnajst (16) istočasnih pogovorov, medtem ko je za prenos podatkov mogoče uporabiti tri (3) repetitorje s po dvema časovnima oknoma, kar pomeni šest (6) istočasnih podatkovnih komunikacij.

Vsaka od lokacij baznih radijskih postaj je lahko glede na število repetitorjev opremljena asimetrično, kar pomeni, da kjer se pričakuje večja prometna gostota govornih in/ali podatkovnih zvez, se planira večje število repetitorjev, kjer pa teh pričakovanj ni oz. je pričakovana majhna gostota, pa se planira temu ustrezno tudi manjše število repetitorjev.

Za pokrivanje celotnega geografskega področja Republike Slovenije bi bilo potrebno sistem realizirati na sedeminpetdesetih (57) lokacijah baznih radijskih postaj. Posamezna lokacija bi bila opremljena asimetrično glede na število repetitorjev na posamezni lokaciji. Minimalno število dupleksnih frekvenčnih kanalov v medsebojnem razmiku 12,5 kHz bi bilo 64, pri čemer je upoštevana rombska razdelitev na nivoju države in geografska razgibanost, ki dopušča pogostejše ponavljanje frekvenc.



Slika 2: Lokacije baznih radijskih postaj ZARE DIGITAL

III. ZAKLJUČEK

Osnovni in največji ekonomski učinki nadgradnje po našem predlogu so na terminalski opremi, saj je potrebno le doprogramiranje z novim frekvenčnim obsegom, kar predstavlja zanemarljiv strošek ali celo nobenega stroška.

Bazne radijske postaje je potrebno nadgraditi z licenčnim programom oz. za nabavo novih predvideti tudi strošek licence.

Infrastruktura ostane za lokacijo ista, le medsebojna povezava IP med baznimi radijskimi postajami v posamezni regije je nov strošek.

Po grobi analizi stroškov je cena nadgradnje oziroma tehnične opreme za prehod v digitalizacijo snopovnega sistema ZARE DIGITAL približno 1 milijon evrov.

Prihodnost DMR komunikacij v sistemu ZARE

Gregor Ščavničar, Dejan Volk, Milan Vrbič, KOMPAS Telekomunikacije d.o.o., Ljubljana

Povzetek — Ta članek opisuje možne implementacije naprednejših DMR radijskih omrežij, za potrebe telekomunikacijske infrastrukture ZARE. Poleg pregleda potrebne strojne opreme in načina delovanja posameznega sistema je v članku govora še o prednostih, ki jih posamezen sistem nudi.

Ključne besede — repetitor, DMR, zveze, RF

Abstract — This article describes the possibilities of implementing advanced DMR radio systems for the needs of ZARE telecommunications infrastructure. Besides the needed hardware, overview of the individual system, there is also talk about the advantages of a specific system.

Keywords — repeater, DMR, communications, RF

I. UVOD

V Sloveniji deluje enoten sistem radijskih zvez v sklopu zaščite in reševanja (ZARE), ki ga uporabljajo reševalne službe, poklicni in prostovoljni gasilci. Sistem ZARE je sestavljen iz hrbteničnega omrežja oziroma baznih postaj in terminalne opreme (ročnih ali mobilnih radijskih postaj). Trenutno je v sistemu 40 analognih baznih postaj in 56 digitalnih baznih postaj [1]. Razlika med omenjenima tipoma postaj je v potencialnih sistemih, ki se lahko tvorijo in v boljše izkoriščeni pasovni širini. Med tem, ko analogni repetitorji nudijo le konvencionalni način komunikacije (postaja – repetitor – postaja), lahko z digitalnimi repetitorji ustvarimo sisteme, ki ne le nudijo "nevidno" prehajanje med bazami (*angl.: roaming*), temveč omogočajo tudi funkcionalnosti, ki so vezane na prenos podatkov (lokacija GPS, tekstovno sporočanje, dodeljevanje nalog …).

Menjava analognih repetitorjev za digitalne bi na področju sistema radijskih zvez ZARE pomenila, da bi se lahko tvorili kompleksnejši sistemi, kot so na primer IP SITE CONNECT (*kratica: IPSC*), Linked Capacity Plus (*kratica: LCP)* in sistem Capacity Plus. Članek predstavlja primerjavo ter prednost posameznih sistemov v korist končnemu uporabniku in posledično izboljšavo komunikacije na področju informacijske in telekomunikacijske tehnologije.

II. TIPIČNE TOPOLOGIJE

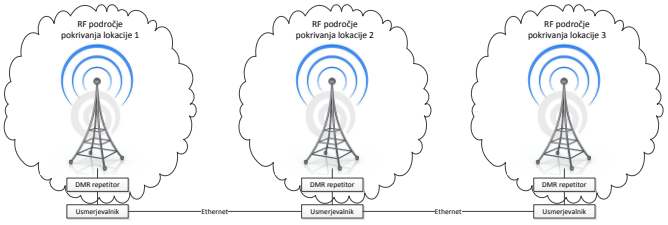
Radijske zveze v digitalnem načinu dela omogočajo več funkcionalnosti kot v analognem. Prvi pogoj za uporabo digitalnega sistema je ustrezna infrastruktura. Za sistem radijskih zvez ZARE so najbolj primerne tri topologije, pri čemer je vsaka naslednja opisana topologija nadgradnja predhodne. Seveda z nadgradnjo na kompleksnejši sistem izgubimo na preprostosti postavitve in vzdrževanju omrežja, vendar pridobimo na uporabi radijskih zvez. V nadaljevanju sledi pregled vseh treh topologij.

A. IP SITE CONNECT

Digitalna topologija IP Site Connect ali kratko IPSC, je najosnovnejša različica vezave DMR repetitorjev. Sistem se uporablja zato, da se repetitorje razpršene na več različnih lokacijah poveže med seboj in se tako ustvari do dva logična kanala. V tem načinu repetitorji med seboj izmenjujejo zvočne in podatkovne pakete po ethernet omrežju. Tak sistem je primeren za povezavo repetitorjev na oddaljenih lokacijah (kjer neposreden RF prehod med njimi ni mogoč), za povečanje RF dometa DMR omrežja in za omogočanje izmenjave podatkov med frekvenčno različnimi omrežji (VHF in UHF).

Glavna prednost in hkrati glavna ovira takega omrežja je, da se ob vzpostavitvi nove zveze na enem izmed logičnih kanalov aktivirajo vsi repetitorji v mreži. V praksi to pomeni, da so v času ene zveze vsi repetitorji v mreži zasedeni – ena sama zveza naenkrat. Iz tega dejstva lahko sklepamo, da je doseg radijskega sistema IPSC enak vsoti dosegov vseh repetitorjev povezanih v mrežo.

Za delovanje sistema sta potrebna vsaj dva digitalna DMR repetitorja, LAN povezava med razpršenimi lokacijami in usmerjevalnik na vsaki strani. Sistem deluje tako, da se med repetitorji tvori mreža IPv4, preko katere se posredujejo paketi TCP/IP na vse repetitorje v mreži.



Slika 1: Topologija IP SITE CONNECT

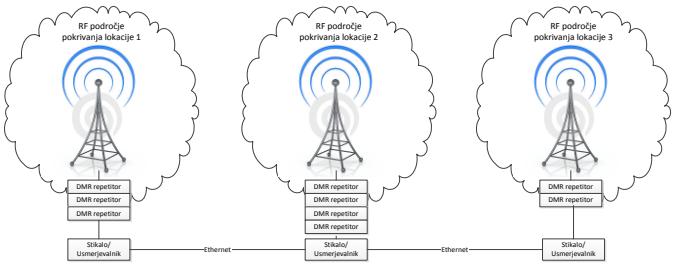
Uporabniki takega omrežja lahko koristijo vse funkcionalnosti, ki so na voljo ob uporabi enega samega digitalnega repetitorja: skupinski klic, individualni klic, tekstovno sporočanje, GPS pozicioniranje, poleg tega pa lahko koristijo še nevidno prehajaje med repetitorji. Za uporabnika to pomeni, da mu znotraj pokrivanja takega omrežja ni potrebno fizično premikati kanalov na radijski postaji, temveč za to poskrbi sistem.

B. LINKED CAPACITY PLUS

Nadgradnja radijskega sistema IPSC je radijski sistem LCP. V tem načinu, enako kot pri IPSC, repetitorske postaje na razpršenih lokacijah med seboj povežemo preko hrbteničnega ethernet omrežja, preko katerega se izmenjujejo paketi TCP/IP. Sistema se razlikujeta v tem, da je na eni lokaciji lahko kaskadno vezanih več repetitorjev in da se lahko ob vzpostavljanju mreže določi točno kateri repetitor se

aktivira ob začetku določene zveze. Ti dve lastnosti tako omogočata, da se poveča kapaciteta prostih kanalov in da se viri koristijo učinkoviteje.

Kaskadna vezava repetitorjev in pravilna konfiguracija leteh deluje tako, da se ob pričetku zveze zasede eden izmed kanalov, ki je na voljo na tej lokaciji. Vsi pripadniki te skupine na tem kanalu, avtomatično prejmejo klic, med tem, ko ostali uporabniki, lahko zasedejo naslednji prost logični kanal.



Slika 2: Topologija LINKED CAPACITY PLUS

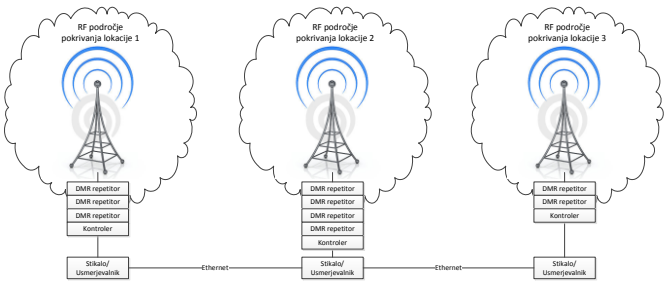
Prednost sistema LCP je v tem, da iz prehoda z IPSC ni potrebna nikakršna dodatna infrastruktura. Edino kar je nujno, so ustrezne licence, ki omogočajo, da repetitorji in terminali (ročne in mobilne radijske postaje) delujejo v takem načinu.

Uporabniki takšnega omrežja, v primerjavi z IPSC, pridobijo na kapaciteti kanalov. V praksi to pomeni, da bi uporabniki manjkrat prejeli zaseden ton ob poskusu vzpostavitve zveze, saj bi bilo na taktičnih lokacijah lahko postavljenih več repetitorjev vezanih v kaskado. Kapacitete le teh bi bile porazdeljene med vse uporabnike v mreži.

C. *CONNECT PLUS*

Najbolj napredna topologija, ki jo trenutno nudi DMR omrežje je sistem Connect Plus. Lastnosti, ki so unikatne za sistem Connect Plus so: dinamično aktiviranje lokacij glede na prisotnost registriranih uporabnikov, preverjanje unikatne ID-številke uporabnika, preverjanje unikatnih ID-številk skupin, omejevanje dostopa, govorne prioritete, čakalna vrsta zvez in shranjevanje ter kasnejše posredovanje tekstovnih sporočil.

Sistem, tako kot prejšnja dva, potrebuje hrbtenično ethernet omrežje, poleg tega pa je na vsaki lokaciji nujen še t.i. kontroler.

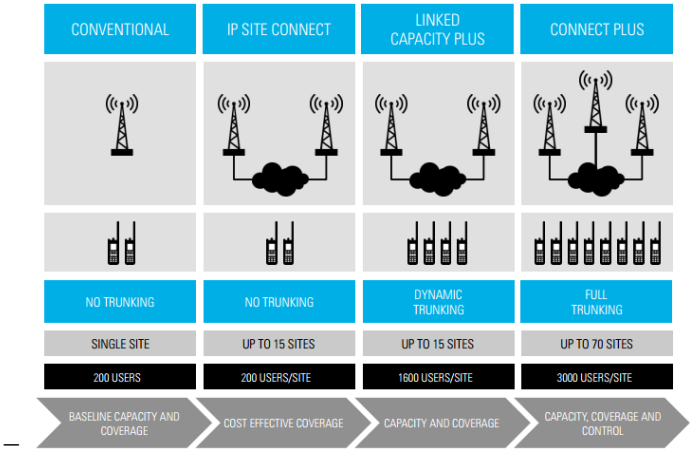


Slika 3: Topologija CONNECT PLUS

Ob vzpostavitvi zveze se mora radijska postaja najprej registrirati v kontrolerju. Registracija se opravi preko kontrolnega kanala in se izvrši samodejno, ko se postaja prižge, ko prehaja med omrežji (t.i. roaming) ali zamenja govorno skupino. V primeru da kontroler ugotovi, da je postaja vpisana v sistem in ima omogočene ustrezne pravice, lahko ta postaja prične oddajati. Podoben proces se izvrši, ko uporabnik postajo izklopi. Postopek deregistracije radijskemu sistemu omogoča, da učinkoviteje izkoristi svoje vire.

III. PRIMERJAVA TOPOLOGIJ

V spodnji tabeli je prikazana primerjava med konvencionalnim načinom delovanja in vsemi tremi opisanimi topologijami. Iz primerjave je razvidno, da se z naprednejšimi topologijami lahko povečuje število podprtih razpršenih lokacij in logičnih kanalov, narašča število uporabnikov, ki jih sistema podpira, poleg kapacitete pa se izboljšuje še koriščenje sistemskih virov.



Slika 4: Primerjava topologij

V nadaljevanju sledi pregled prednosti topologije LCP glede na IPSC:

- več logičnih kanalov na posamezni lokaciji,
- dinamično dodeljevanje logičnih kanalov,
- do osem krat več uporabnikov na lokacijo*.

Prednosti topologije Connect Plus glede na LCP:

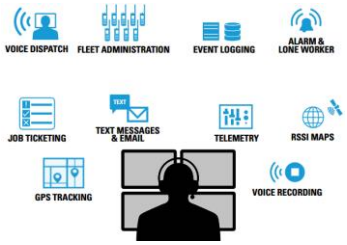
- več lokacij (do sedemdeset*),
- avtentikacija uporabnikov,
- kontrolni kanal – hitrejša odzivnost,
- do 420 repetitorjev v sistemu*,
- do 3000 uporabnikov na lokacijo*.

*velja za različico programske opreme 1.5

IV. USKLAJEVANJE DEL – DISPEČER

Digitalizacija radijskih zvez je omogočila tudi razširitev sposobnosti radijskih postaj. DMR danes poleg prenosa govora omogoča prenos lokacijskih informacij, sporočil SMS, samodejna prijava v sistem zaznavanja prisotnosti radijske postaje v omrežju, telemetrije in klasičen prenos datotek preko radijske mreže.

Omenjene funkcionalnosti so omogočile razvoj naprednejših dispečerskih centrov nove generacije, ki organizacijam ponujajo izvajanje različnih opravil na radijskem omrežju, ki pred tem niso bila mogoča.



Slika 5: Dispečerski center

A. *Zvočne storitve*

Digitalizacija radijskega omrežja je prinesla tudi nove možnosti na področju glasovne komunikacije. Dispečerji lahko sedaj s pomočjo nove generacije dispečerskih centrov izvajajo zasebne klice, v katerega sta udeležena samo dispečer in poklicana radijska postaja, pri čemer ostali člani skupine pogovora ne slišijo. Dispečer lahko izvede tudi t.i. alarmni poziv, pri čemer na klicani radijski postaji sproži alarm v obliki zvonjenja, s čimer opozori uporabnika omenjene postaje, da je prejel zasebni klic.

B. *Lokacijske storitve*

Lokacijske storitve omogočajo pridobitev lokacijskih podatkov GPS za vsako digitalno radijsko postajo v omrežju DMR. Možni načini pridobitve lokacijskih podatkov so predvsem:

- takojšnja, enkratna pridobitev, kjer dispečerski center odda zahtevo poljubni radijski postaji v omrežju po pridobitvi lokacijskih podatkov
- periodična pridobitev, kjer radijska postaja v dispečerski center oddaja podatke o lokaciji glede na časovno periodo (npr. 60 sekund)
- intervalna pridobitev glede na razdaljo, kjer radijska postaja pošlje podatek o lokaciji na vsakih N metrov,
- posredovanje lokacijskih podatkov ob zunanjih dogodkih, kjer radijska postaja pošlje podatek o lokaciji ob zaznavanju zunanjih dogodkov, npr. odpiranje vrat avtobusa, zagon motorja vozila
- posredovanje lokacijskih podatkov ob potencialni življenjski ogroženosti, npr. klic v sili, zaznavanje padca postaje (t.i. funkcija "Man Down")

Omenjeni načini se uporabljajo za nadzor uporabnikov radijskih postaj, kar olajša koordinacijo razpoložljivih enot na terenu. Poleg tega lahko moderni dispečerski sistemi omogočajo t.i. "geofencing", kjer dispečerski center samodejno opozori dispečerja, da je neka radijska postaja zašla iz omejenega področja gibanja, ki jo je dispečer oz. administrator sistema vnaprej določil. Dispečerski centri omogočajo tudi rekonstrukcijo prepotovane poti, kar olajša analizo akcij posameznih enot in dogodkov po zaključenem posredovanju.

C. *Sporočila SMS*

Radijske postaje DMR omogočajo tudi izmenjavo sporočil SMS, ki so lahko naslovljeni na posameznika (posamezno ID številko) ali celotni radijski skupini hkrati. Dispečerski centri lahko pošiljajo posamezna ali skupinska sporočila SMS na vse delovne kanale, pri čemer lahko uporabniki radijskih postaj odgovarjajo na sporočila SMS.

Določeni proizvajalci radijske opreme omogočajo tudi uporabo sistema dodeljevanja delovnih nalogov (komercialno ime "Job ticketing"), kjer dispečerji uporabnikom radijskih postaj dodeljujejo delovne naloge, ki jih nato uporabniki sprejmejo ali zavrnejo ter ob zaključku naloge obvestijo dispečerja o opravljenem delu.

D. *Telemetrija*

Storitev telemetrije se nanaša na analizo oz. uporabo zunanjih virov, ki so lahko priključeni na radijsko postajo, v primeru, da le-ta omogoča priklop t.i. vmesnika GPIO ali General Purpose Input/Output. Dispečer nato lahko s pomočjo storitev telemetrije nadzira stanje teh naprav ali neposredno vpliva na njihovo delovanje, npr. odpiranje prednjih garažnih vrat gasilskega doma, odpiranje ali zapiranje zapornic, pridobivanje meritev napetosti baterij na oddaljeni lokaciji itd.

E. *Zaznavanje prisotnosti radijskih postaj v omrežju*

Omrežje DMR omogoča tudi samodejno prijavo radijske postaje v dispečerski center s pomočjo sistema za zaznavanje prisotnosti radijske postaje v omrežju. Radijska postaja obvesti center o svoji prisotnosti ob vžigu, ob menjavi kanala ali cone in ob izklopu. Poleg tega lahko tak sistem omogoča tudi ločeno prijavo uporabnika v radijski sistem, kar je uporabno predvsem takrat, kadar si radijsko postajo deli več različnih uporabnikov.

F. *Pošiljanje alarmov v sili/klic v sili*

Tehnologija DMR omogoča tudi pošiljanje kritičnih podatkov, ki se aktivirajo ob izrednih dogodkih. Primeri takih dogodkov je t.i. funkcija "Man Down", pri katerem ima postaja v sebi vgrajen merilec pospeška in žiroskop, pri čemer proži alarm v primeru, da zazna prekomerne pospeške in/ali nenavadno lego radijske postaje. Poleg tega dispečerski centri lahko v primeru, ko uporabnik sam ali njegova radijska postaja proži klic v sili in se uporabnik ne odzove na klice dispečerja, lahko le-ta na daljavo aktivira mikrofon ter posluša dogajanje okoli radijske postaje. Poleg tega lahko dispečerski centri samodejno nastavijo zahteve po pridobitvi lokacije radijske postaje tako, da ukažejo radijski postaji, naj ob izrednih dogodkih samodejno pošlje koordinate v dispečerski center.

G. *Izmenjava datotek preko radijskega omrežja*

Ker omrežje DMR temelji na omrežni tehnologiji, ki se danes uporablja v računalniških omrežjih, je možno enostavno prenašati poljubne datoteke iz ene radijske postaje na drugo s pasovno širino, ki jo omogoča frekvenčno področje VHF.

V. ZAKLJUČEK

Glede na pregled topologij in uporabo radijskih zvez v Sloveniji je razvidno, da je naslednji smiseln korak za sistem ZARE postavitev vsaj sistema Linked Capacity Plus (LCP).

Ob vzpostavitvi sistema LCP bi končni uporabnik to občutil kot višjo razpoložljivost (sistem redkeje zaseden) in prosto prehajal med lokacijami. Ob ustrezni konfiguraciji sistema in terminalne opreme bi lahko uporabniki komunicirali le z osebami oziroma organizacijami, ki bi bile za njih interesantne. Tako bi zagotovili, da bi se sistem aktiviral le na tistih lokacijah, kjer bi bilo to zanimivo. Poleg tega bi sistem lahko nudil način komunikacije za več skupin

kot zdaj, kar v praksi pomeni, da bi se gasilcem in zdravstvenim domovom lahko priključile še druge javne službe.

V primeru, da bi se v prihodnosti izkazalo, da sistem LCP ne zadostuje potrebam, je mogoč modularen prehod na sistem Connect Plus z dograditvijo infrastrukture – kontrolerji ter dodatna terminalna strojna oprema.

Gregor Ščavničar je leta 2013 zaključil izobraževanje na Fakulteti za Elektrotehniko, smer telekomunikacije. Predhodne delovne izkušnje obsegajo pridobivanje, obdelavo in analizo podatkov radijskega omrežja pri enem izmed mobilnih operaterjev, v oddelku za zagotavljanje kakovosti. Od leta 2013 je zaposlen pri podjetju KOMPAS Telekomunikacije, d.d., kot prodajno/tehnični svetovalec, kjer svetuje končnim uporabnikom in sodeluje pri konstrukciji radijskih omrežij.

Milan Vrbič je leta 2003 diplomiral na Fakulteti za telekomunikacije v Ljubljani. Od leta 2005 je zaposlen v podjetju KOMPAS Telekomunikacije, d.o.o. na mestu tehničnega svetovalca. Zadolžen je za svetovanje, načrtovanje, implementacijo in tehnično podporo profesionalnih radijskih sistemov različnih platform (DMR, TETRA, analogni sistemi, mikrovalovne povezave,…).

Podporniki

Sponzors

Telekom Slovenije

Kapsch

Iskratel

AKOS

ARNES

Univerza v Mariboru, FERI

strokovni

Univerza v Ljubljani, LTFE

strokovni