Daljinski nadzor i izvedeni alarmi – put ka smart mrežama i odgovor na evropske preporuke

Bojana Jovanović, Dragana Petrović, Miroslav Lazić
Sektor za energetsku elektroniku
Iritel a.d. Beograd
Beograd, Srbija
bojanaj@iritel.com, titelac@iritel.com, mlazic@iritel.com

Branko Blanuša
Elektrotehnički fakultet
Univerzitet u Banja Luci
Banja Luka, Republika Srpska
branko.blanusa@etf.unibl.org

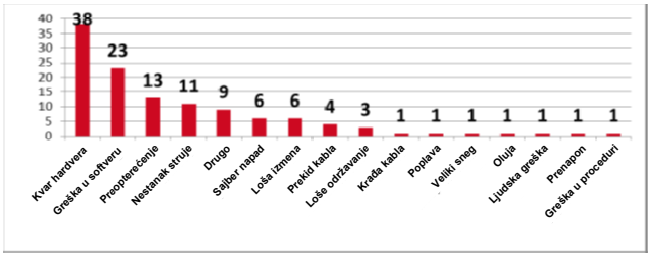
Sažetak—**Reforma pravnog okvira Evropske unije za elektronske komunikacije razmatra sigurnost i integritet elektronskih komunikacionih mreža i usluga. Uređaji energetske elektronike su sastavni element svakog objekta koji služi za prenos telekomunikacionog i informacionog saobraćaja. Pored toga, predstavljaju sastavni deo svakog industrijskog procesa. Uređaji energetske elektronike obezbeđuju rad većeg broja različitih uređaja i zajedno sa uređajima koje napajaju čine sistem. Sistemi mogu biti pod direktnim nadzorom službi održavanja, ali mogu biti značajno udaljeni od službi koje kontrolišu ispravnost rada sistema. Za udaljene sisteme neophodno je organizovati daljinski nadzor i upravljanje, na način koji je ovim službama najpodesniji. U tu svrhu, predlažu se izvedeni alarmi, koji idu korak dalje i daju preporuke sačinjene na osnovu ekspertskog znanja.**

Ključne riječi-daljinski nadzor; izvedeni alarmi; evropske preporuke; energetska elektronika;

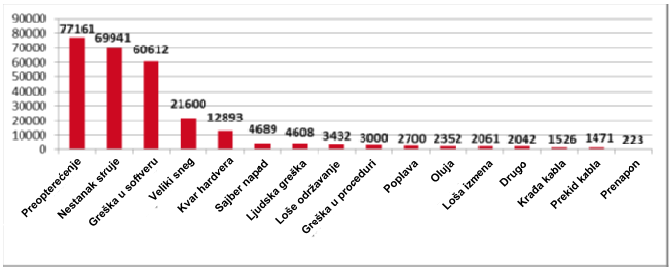
I. UVOD

Reforma pravnog okvira Evropske unije za elektronske komunikacije, koja je usvojena 2009. godine i stupila na snagu maja 2011. godine, dodaje Član 13a Okvirnoj direktivi 2009/140/EC o elektronskim komunikacijama [1]. Član 13a razmatra sigurnost i integritet javnih elektronskih komunikacionih mreža i usluga, i u njemu se navodi da pružaoci javnih komunikacionih usluga moraju da primene mere zaštite kojima bi garantovali sigurnost i integritet svojih mreža (na primer, fiksna i mobilna telefonija, fiksni i mobilni internet pristup). Prema ENISA (eng. „European Union Agency for Network and Information Security (ENISA)“) [2], čak manje od polovine članica Evropske unije je primenilo potrebne zaštitne mere. U cilju primene Člana 13a, Nacionalne regulatorne agencije članica Evropske unije, imaju obavezu da izveštavaju o incidentima sa značajnim uticajem na elektronske komunikacione mreže i usluge. Svake godine, Agencija Evropske unije za mreže i sigurnost informacija (ENISA), objavljuje godišnji izveštaj, kojim se sumiraju prijavljeni incidenti i prikazuje sveobuhvatna analiza i rezultati. U Srbiji je ova tematika uređena Zakonom o elektronskim komunikacijama [3].

U izveštaju ENISA [2], može se videti da su prekidi napajanja dominantan uzrok ozbiljnih prekida rada mreža i prekida usluga u sektoru elektronskih komunikacija. U izveštaju se takođe navodi da postojeći nivo zaštite od prekida napajanja nije dovoljan [2]. Upotreba solarnih panela i sličnih tehnologija može pružiti veliku pomoć, ali takođe uglavnom nije u upotrebi [2]. Na slici 1 je prikazana detaljna analiza uzroka prekida elektronskih komunikacionih usluga, dok je na slici 2 prikazan uticaj pojedinih uzroka incidenata na korisničke sate [2].



Slika 1. Uzroci incidenata (%) [2]



Slika 2. Uticaj uzroka incidenata na korisničke sate (u hiljadama) [2]

ENISA izveštaji o incidentima iz 2012. i 2011. godine [4], [5] prikazuju da značajan broj prekida napajanja koji su doveli do ozbiljnih narušavanja usluga, ne bi doveli do ozbiljnih posledica, ukoliko bi mere zaštite odgovarajuće funkcionisale. U izveštaju [2] se navode zaključci koji se odnose na prekide napajanja i njihove uzroke: prekidi napajanja su 2011. godine identifikvani kao drugi najveći uzrok incidenata; tokom 2012. godine su prekidi napajanja bili četvrti najčešći uzrok; prekidi napajanja su u 2012. godini imali ogroman uticaj na gubitak

korisničkih sati po incidentu; tokom 2012. godine incidenti uzrokovani prirodnim pojavama (uglavnom oluje i veliki sneg) su bili jedni od glavnih uzroka velikih incidenata koji su trajali do 36 sati; tokom 2011. godine su prirodne pojave prouzrokovale incidente koji su u proseku trajali 45 sati [2].

U skladu sa preporukama koje navodi ENISA [2], pružaoci komunikacionih usluga treba da sprovode provere postojećih mera zaštite, među kojima su i provere UPS sistema i baterija. Međutim, bitan faktor je i svest o potrebi za razmenom informacija, među različitim akterima. Neke od najčešćih mera zaštite koje se primenjuju su redundantnost hardvera, nabavka agregata, planiranje i nadzor napajanja, kao i mere fizičke zaštite [2]. Opšte pravilo je da bazne stanice imaju neki vid UPS sistema u upotrebi. U ruralnim predelima, gde postoji samo nekoliko korisnika na koje može uticati prekid usluge, ne postoji ovakva praksa. Međutim, u naseljenijim krajevima, rezervno napajanje mora da pruži najmanje 4-6 sati kontinuiranog rada.

Osnova prevencije i ublažavanja negativnih efekata prekida napajanja je sprovođenje sveobuhvatne procene rizika i pravljenje plana za kontinuitet poslovanja (regulisan standardom ISO 22301 [6]). Osnova za to je analiza učestalosti i uticaja prekida napajnja na prekide u mrežama i uslugama. Postoji četiri vrste lokacija, u zavisnosti od mrežne opreme koja je na njima montirana – klase A, B, C i D [2]. Za lokacije klasa A i B, rezervno napajanje mora biti dovoljno za najmanje tri dana. Za lokacije klase C je neophodno rezervno napajanje za dva dana, a za lokacije klase D ne postoji specificiran zahtev za rezervno napajanje. Takođe, mobilne mreže treba da budu u mogućnosti da pružaju usluge (i govor i podaci) najmanje šest sati posle nestanka primarnog napajanja. Finskom regulativom propisano je da GSM bazne stanice moraju imati rezervno napajanje za bar tri sata, a ovo vreme se produžava na šest sati za udaljene lokacije, nepristupačne terene i kada se očekuju loši vremenski uslovi [7]. Napajanje je kritični faktor u sektoru elektronskih komunikacija. Zbog toga je veoma značajno redovno nadzirati rad uređaja koji obezbeđuju napajanje.

U nastavku je ukratko opisana struktura rada prema pojedinačnim poglavljima. U uvodu je ukratko prikazana regulativa i evropske preporuke koje ukazuju na potrebu za daljinskim nadzorom i formiranjem izvedenih alarma, kojima je tema ovog rada i motivisana. U drugom poglavlju je opisan način obrade podataka u centrima za nadzor, dok je poglavljem tri detaljnije prikazana organizacija daljinskog nadzora i upravljanja. Definicija pojma „izvedeni alarmi“ i njihovog značaja za službe održavanja se nalazi u poglavlju četiri, dok su u poglavlju pet dati zaključak rada i smernice za buduće istraživanje.

II. OBRADA PODATAKA U CENTRIMA ZA DALJINSKI NADZOR I UPRAVLJANJE

Za službe održavanja od vitalne važnosti je da u svakom trenutku imaju informaciju kako funkcionišu sistemi koje održavaju. Da bi se ta funkcija ostvarila, neophodno je da postoje uređaji za prikupljanje relevantnih podataka o sistemu i telekomunikacioni kanal preko koga se prikupljeni podaci mogu poslati do nadležnih službi. Postoje brojni pretvarači električnih i neelektričnih veličina u električne signale pogodne za prenos kroz telekomunikacione mreže. Savremene mreže za prenos podataka omogućavaju brz i pouzdan prenos podataka. Uređaji za daljinski nadzor i upravljanje prikupljaju i obrađuju podatke o svim relevantnim veličinama. Prikazuju ih u formi koja je potrebna nadležnim službama, da pruži precizan uvid u fukcionisanje sistema, i na taj način, postaju obavezan element svih sistema. Podaci o skupu izmerenih veličina, prosleđuju se u jedan ili više centara za nadzor. U centrima za nadzor se, na osnovu dobijenih podataka, odlučuje o intervenciji nad nadziranim sistemima.

U jednoj organizaciji koja se bavi prenosom podataka, može postojati i veliki broj uređaja energetske elektronike. U jednoj regionalnoj telekomunikacionoj oraganizaciji broj perifernih uređaja je oko hiljadu. Svaki od tih uređaja ima mogućnost slanja alarma (različitih prioriteta) i merenja električnih i neelektričnih veličina. Nadzorne službe su „zatrpane“ velikim brojem podataka. Obrađuju se samo alarmi najvišeg prioriteta, dok se ostali alarmi i merenja obrađuju samo ukoliko postoji slobodno vreme. S druge strane, kompanije smatraju da im ovakva savremena oprema omogućava smanjenje broja zaposlenih, tako da je često u službama održavanja uređaja energetske elektronike samo 2-3 radnika zaduženo za održavanje više od 1000 uređaja. Praktično, ne postoje analize rada pojedinih sistema koji nisu u alarmu, sa ciljem da se preduprede prekidi rada uređaja energetske elektronike, koji kao posledicu imaju prekid prenosa podataka.

Jedan od načina otklanjanja opisanih problema jeste formiranje odgovarajućih filtara, koji će smanjiti broj alarma koji se prosleđuju službama održavanja. Pored toga, mora postojati i višeslojna hijerarhija, koja omogućava da se odgovarajući skup podataka prosledi ka nadležnim službama, u odgovarajućem obimu. Dakle, postavlja se nekoliko važnih pitanja za kreiranje organizacije daljinskog nadzora i upravljanja prikupljenim podacima. Kako treba prikupljati podatke? Kome je potrebno slati prikupljene podatke? U kojoj formi je potrebno prezentovati prikupljene podatke, i da li se forma razlikuje u zavisnosti od korisnika podataka?

III. ORGANIZACIJA DALJINSKOG NADZORA I UPRAVLJANJA

Daljinski nadzor i upravljanje se organizuje na različite načine. Jedna podela može biti na:

- ***Centralizovan (direktan) nadzor;*** Svi periferni uređaji šalju alarme i podatke u jedan centar za nadzor. Glavni centar za nadzor prikuplja podatke o radu svih uređaja u sistemu. Na osnovu primljenih alarma iz centra za nadzor se šalju poruke nadležnim službama održavanja koje otklanjaju probleme u radu uređaja.
- ***Posredan nadzor;*** Podaci o radu svake grupe perifernih objekata se šalju ka najbližim službama održavanja te grupe uređaja, zatim ka ekspertskim centrima za tu vrstu uređaja. Na kraju se šalju u glavni centar za nadzor, u kome se kontroliše rad svih uređaja u sistemu.

U praksi je više rasprostranjen centralizovan nadzor. Brojni su razlozi za to. Za rukovodioce koji globalno prate sistem, najvažniji podatak je da li sistem funkcioniše. Naravno,

zanima ih koji deo sistema ne funkcioniše ispravno. Pri tome, sam razlog neispravnog rada nije od krucijalnog značaja. Pored toga, centralizovan nadzorni sistem je jednostavan za realizaciju. Pošto periferni uređaji šalju poruke direktno glavnom centru (u praksi se obično naziva nacionalni centar) za nadzor, ne postoji mogućnost da poruka ne stigne tamo gde je i poslata. To je i najjeftiniji način organizovanja daljinskog nadzora i upravljanja. S obzirom na raznovrsnost poruka koje stižu u glavni centar, u glavnom centru ne rade ekeperti, već službenici koji će na bazi dobijenog alarma prosleđivati odgovarajuću poruku iz baze podataka nadležnim službama održavanja.

Nedostaci ovakvog pristupa su brojni. Prvo, u glavnom centru se nadzire veliki broj različitih uređaja. Broj alarma koji dolazi je veoma veliki. Praktično, glavni centar je zatrpan alarmima i upozorenjima. Da bi se taj problem rešio, podaci se filtriraju i realno je da se pri tome izgube i podaci koji su važni za rad sistema. I pored toga, broj podataka je preveliki, pa se službenici koncentrišu na alarme najvišeg prioriteta. To znači da se neće postupati po upozorenjima i sprečavati nastajanje štete, već će intervencije nadležnih službi biti samo na otklanjanju posledica, odnosno smanjivanju štete koja svakako postoji. Preventivnog održavanja nema. Praktično, cilj je da se minimiziraju negativni efekti problema. Službe održavanja dobijaju naloge za intervencije (tikete) na koje moraju da odgovore. Praksa pokazuje da su u velikom procentu njihove intervencije neuspešne. Odlaskom na periferni objekat utvrde da je uzrok u otkazu nekog drugog elementa u sistemu za koji nisu nadležni. Zatim na objekat odlaze službe održavanja druge grupe uređaja. Ovakvi problemi bi se izbegli kada bi podatke o upozorenjima i alarmima analizirale službe održavanja za tu grupu uređaja. Međutim to se ne uklapa u koncepciju centralizovanog nadzora.

Teorijski, ukoliko bismo napravili da svi periferni objekti do detalja budu identični, da rade svi u jednakim eksternim uslovima, mogao bi se formirati centralizovan sistem za nadzor, kod koga bi se otklonila većina opisanih nedostataka. Nažalost, to je u praksi nemoguće ostvariti.

Kod posrednog nadzora se podaci od perifernih uređaja prosleđuju do lokalnih službi održavanja. Set podataka koji prate lokalne službe održavanja je najveći. Pored alarma, prikupljaju se i obrađuju podaci o upozorenjima, kao i periodično prikupljena merenja relevantnih veličina (tzv. „kontinualni nadzor“). S obzirom na to da je broj perifernih uređaja na lokalnom nivou daleko manji od broja uređaja kod centralizovanog nadzora, moguće je obraditi na pravi način sve prikupljene podatke. Praktično, moguće je praćenje rada perifernih uređaja u realnom vremenu i pre prekida prenosa podataka preventivno intervenisati. Lokalne službe održavanja detaljno poznaju sve periferne uređaje koje nadziru, pa mogu optimizirati sve neophodne intervencije. Za lokalne službe održavanja je važno koji od nadziranih uređaja ne funkcioniše ispravno, šta je izazvalo otkaz uređaja, kao i moguće neispravnosti na uređaju, čak i kada je on u funkciji. Na taj način, služba održavanja pre nego što ode na lokaciju, ima pouzdane podatke o problemu koji mora da rešava. To omogućava efikasniji rad službi održavanja (planiranje resursa). Smanjuju se troškovi i potrebe za angažovanjem zaposlenih.

Lokalni nadzorni centri prosleđuju deo podataka ka višem nivou nadzora specifične grupe uređaja. Obično postoji jedan takav centar i često se naziva ekspertski centar. U ekspertskom centru se prati rad na celoj teritoriji nekog korisnika. Na osnovu prikupljenih podataka se sugeriše lokalnim centrima o neophodnim intervencijama, kojima se povećava pouzdanost rada celog sistema koji se nadzire.

Set podataka prikupljenih u lokanim nadzornim centrima se prosleđuje u glavni centar za nadzor. Glavni centar za nadzor je i dalje neophodan, jer je to jedini centar za nadzor koji funkcioniše neprekidno. Međutim, set podataka je tako filtriran, da se lokalne službe održavanja angažuju samo kada je to neophodno i kada će to dovesti do otklanja prekida telekomuniakcionog saobraćaja.

Osnovna prednost posrednog nadzora je što odluke o intervenciji donose tehnička lica specijalizovana za održavanje opreme koja se nadzire. Pored toga što poznaju opremu koju održavaju, poznaju i lokacije objekata i najbolje načine kako da otklone uočene nedostake. Takođe, kontinualan nadzor omogućava preventivno održavanje, što je krajnji cilj svih sistema za nadzor i upravlajnje.

Nedostatak je složenost sistema. Postoji veća mogućnost da se u nekoj stepenici hijerarhije izgube neki podaci, pa da se i ne pojave u glavnom centru za nadzor.

Ovakav pristup nije omiljen u organizacijama koje su tako napravljene da se sve odluke donose sa najvišeg nivoa. Međutim ekonomska korist koja će se ostvariti preventivnim održavanjem bi trebalo da nadvlada strogu hijerarhiju.

IV. IZVEDENI ALARMI - POMOĆ SLUŽBAMA ODRŽAVANJA

Sistemi za daljinski nadzor i upravljanje su postali neophodni u sistemima i primenjuju se već više od 20 godina. U početku je bilo važno znati da li svi elemeti sistema funkcionišu, kasnije i kako funkcionišu, dok se danas očekuje da se preventivnom intervencijom spreči prekid u funkcionisanju nadziranog sistema. Jedan od elementa preventivnog održavanja je nazvan ***Izvedeni alarm***.

U radu [8] je definisan pojam „izvedeni alarmi“. Izvedeni alarmi su nastali kao preporuka grupe autora, nakon razvoja i montaže velikog broja nadzornih sistema i analize postignutih rezultata. Analizirani su rezultati rada oko 300 sistema, u periodu od 15 godina.

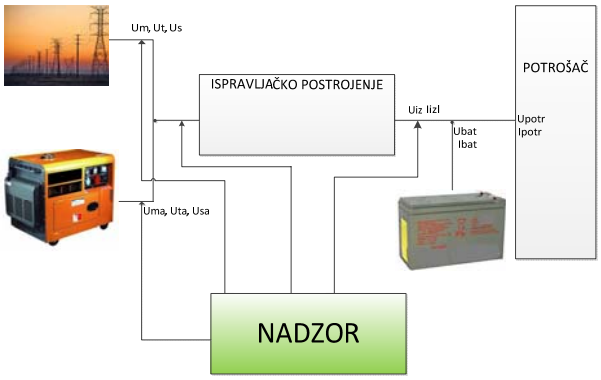
Izvedeni alarmi nastaju na bazi alarma i izmerenih veličina na perifernim objektima. Algoritme za generisanje izvedenih alarma definišu nadležne službe za održavanje nadziranog sistema. Generišu se na osnovu skupa podataka:

- Podaci o objektu koji se nadzire, značaj objekta, udaljenost od službi održavanja, pristupačnost objekta,
- Tehnički podaci o opremi koja se nalazi u nadziranom objektu,
- Podaci iz baze podataka, formiranih od strane nadzornih sistema u prethodnom perodu,
- Podaci iz iskustva kod prethodnih intervencija na nadziranom objektu.

Jasno je da formiranje algoritama za generisanje izvedenih alarma zahteva izuzetno znanje i značajno iskustvo. Može se reći da algoritme za izvedene alarme generišu eksperti za pojedine grupe uređaja. Znanje i iskustvo u korišćenju sistema za nadzor može se iskoristiti za poboljšanje sadržaja informacija koje se šalju ka glavnom nadzornom centru. Nekoliko alarma u nizu mogu se sjediniti u jednu poruku i na taj način smanjiti broj poruka. S druge strane, moguće je sugerisati nadležnim službama da preduzmu preventivne intervencije i ako ne postoji alarmno stanje. Dakle, izvedeni alarmi omogućavaju preventivno održavanje.

Izvedeni alarmi omogućavaju formiranje „smart“ (pametnih) mreža za nadzor i upravljanje.

Na slici 3 je prikazana tipična konfiguracija uređaja energetske elektronike na jednom telekomunikacionom objektu. Na slici su obeleženi signali koji se prenose preko nadzornih sistema.

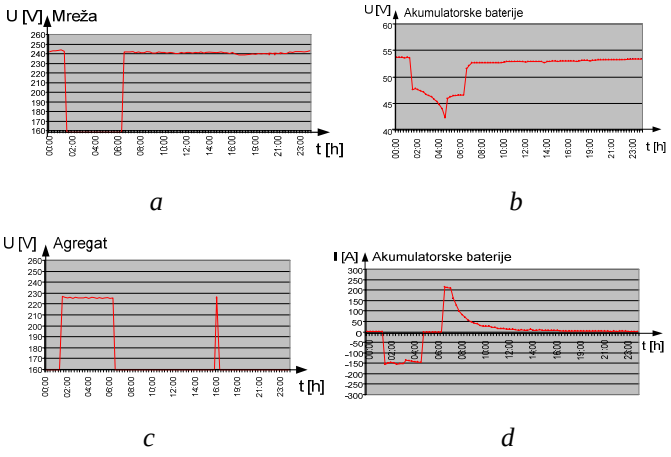


Slika 3. Blok šema povezivanja nadzora u elektroenergetski sistem telekomunikacionog objekta

Ukoliko je prisutan mrežni napon, telekomunikacioni objekat se napaja iz elektrodistributivne mreže. Ukoliko nastane prekid napajanja iz elektrodistributivne mreže, automatski se startuje agregatsko postrojenje. U periodu dok se stabilizuje napon agregata, potrošači se napajaju iz akumulatorskih baterija. Međutim, u praksi se događa da u prelaznom režimu dođe do otkaza neke od energetskih komponeneta, pa iako je agregat regularno startovao, potrošači se i dalje napajaju iz akumulatorskih baterija. Nadzorni sistem pokazuje da nema mrežnog napona i da je agregat ispravno startovao. Međutim, napajanje potrošača je iz akumulatorskih baterija. Vreme rada uređaja kada se napajaju iz akumulatorskih baterija je ograničeno kapacitetom baterija. Ukoliko se ne interveniše, doći će do prekida telekomunikacionog saobraćaja.

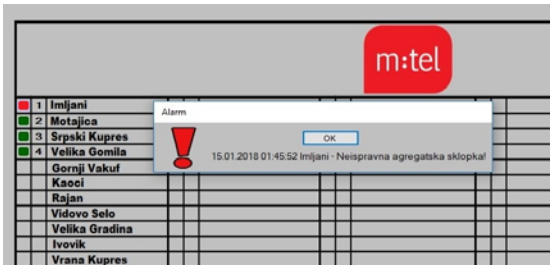
Sistem za daljinski nadzor i upravljanje SDNU služi za nadzor različitih uređaja energetske elektronike. Sastoji se od perifernog uređaja DNU24, centralne jedinice i grafičke aplikacije koji se nalaze u računaru. Komunikacija između periferne i centralne jedinice je omogućena, po namenski razvijenom protokolu SDNU, preko nekoliko prenosnih puteva: *Ethernet*, *GPRS* i *Dial-up*. [9,10,11]. SDNU je nadzorni sistem koji pored digitalnih i analognih alarma generiše i izvedene alarme. Izvedeni alarmi su nastali kao rezultat dugogodišnjeg praćenja i izučavanja sistema energetske elektronike.

Na slici 4 su prikazani dijagrami snimljeni pomoću SDNU u jednom telekomunikacionom objektu. Incident je nastao nakon nestanka mrežnog napona (dijagram *a* na slici 4) i startovao je agregat (dijagram *c* na slici 4). Agregatska sklopka nije ispravna, pa napon agregata nije prosleđen do ispravljačkih postrojenja. Potrošači se napajaju iz baterije. Na slici 4 na dijagramu *b* se vidi kako se smanjuje napon baterije, a na dijagramu *c* struja sa kojom se prazni akumulatorska baterija. Iako je agregat ispravan, baterija se prazni i to dovodi do prekida telekomunikacionog saobraćaja. Veličina struje kojom se prazni baterija vidi se na dijagramu *d*.



Slika 4. Grafici izmerenih vrednosti pre i posle izvedenog alarma: a) Mrežni napon, b) Napon akumulatorske baterije, c) Napon agregata, d) Struja akumulatroske baterije

U ovakvoj situaciji se generiše izvedeni alarm. Pošto nema mrežnog napona, a postoji agregatski napon, ne sme se smanjivati napon akumulatorske baterije. Ukoliko se smanjuje, generiše se izvedeni alarm „***neispravana agregatska sklopka“, a nakon toga poruke „Rad na baterije, vreme rada na baterije xxx minuta“.*** Procena vremena rada na baterije se vrši na osnovu kapaciteta baterije i struje potrošnje. Kapacitet baterije je definisan poslednjom kapacitivnom probom koja je urađena na tom objektu. Podaci o kapacitvnoj probi se unose automatski u bazu podataka sistema za nadzor.



Slika 5. Izvedeni alarm- prikaz na računaru

Opisana situacija, prikazana na slici 4 ne predstavlja alarm jer su sve vrednosti napona i struja u dozvoljenom opsegu. Međutim, ovakva situacija će postati incident onog momenta kada se pojavi alarm da je napon na donjoj granici. Kada će se

pojaviti alarm, zavisi od podešavanja granica alarma. Ukoliko sistem nadzora poseduje izvedene alarme, upozoravajući alarm će se aktivirati nekoliko minuta nakon startovanja agregata. Izvedeni alarm pojavljuje se kao *pop-up* prozor i prikazan je na slici 5. Lokacija na kojoj se pojavio alarm označena je crvenom bojom i korisniku jasno definiše alarmno mesto.

Nakon dobijanja izvedenog alarma, službe održavanja mogu da provere da li će se uspostaviti napajanje iz elektrodistributivne mreže u vremenu rada na akumulatorske baterije. To znači da nije neophodna hitna intervencija. Ili, ako neće doći do uspostave napajanja iz elektrodistributivne mreže, koji stručnjaci moraju ići na intervenciju i koliko vremena imaju za intervenciju. Krajnji cilj je da ne dođe do prekida telekomunikacionog saobraćaja.

V. ZAKLJUČAK

Prekidi napajanja se smatraju jednim od najčešćih uzroka prekida usluga telekomunikacionih kompanija. Identifikovani su kao drugi najveći uzrok prekida usluge i imaju ogroman uticaj na gubitak korisničkih sati u telekomunikacionom saobraćaju. U radu je prikazan jedan pristup rešavanju problema prekida napajanja. Defisan je postupak koji omogućava da se iskoristi znanje i iskustvo službi održavanja za definisanje specifične vrste alarma: ***Izvedeni alarmi***. Izvedeni alarmi su osnova za formiranje smart nadzornih sistema. Smart nadzorni sistemi bi trebalo da omoguće preventivno održavanje uređaja važnih za funkcionisanje sistema. Treba eliminisati mogućnosti koje mogu dovesti do prekida napajanja i na taj način prekida prenosa podataka.

U radu je dat i ilustrativan primer generisanja izvedenog alarma. Broj izvedenih alarma stalno raste i u narednim radovima će biti klasifikovani na bazi višegodišnjeg iskustva.

ZAHVALNICA

Ovaj rad je deo projekta podržanog od strane Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije, sa oznakom III43008 „Razvoj metoda, senzora i sistema za praćenje kvaliteta vode, vazduha i zemljišta“.

LITERATURA

[1] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services

[2] European Union Agency for Network and Information Security (ENISA) Power Supply Dependencies in the Electronic Communications Sector - Survey, analysis and recommendations for resilience against power supply failures, December 2013

[3] Zakon o elektronskim komunikacijama ("Službeni glasnik RS", br. 44/2010, 60/2013 - odluka US i 62/2014)

[4] European Union Agency for Network and Information Security (ENISA) Annual Incident Reports 2011, Analysis of the Article 13a incident reports of 2011, October 2012

[5] European Union Agency for Network and Information Security (ENISA) Annual Incident Reports 2012, Analysis of Article 13a annual incident reports, August 2013

[6] ISO 22301:2012, Societal security – Business continuity management systems – Requirements

[7] Regulation FICORA 57 A/2012 M on the maintenance of communications networks and communications services, procedures and notifications in the event of faults and disturbances, Finnish Communications Regulatory Authority, Helsinki, January 2012

[8] D. Petrović, M. Lazić, B. Jovanović, Z. Cvejić, “Organizacija prenosa podataka u sistemu za daljinski nadzor SDNU”, 57. konferencije ETRAN, ISBN 978-86-80509-67-9, str. EL3.6.1-5, Zlatibor, jun 2013.

[9] Miroslav Lazić, „Daljinski nadzor i upravljanje uređajima energetske elektronike – SDNU“, Zbornik radova 53. EL 1.1, ISBN 978-86-80509-62-4, Konferencije za ETRAN, Vrnjačka Banja, 15-18. Juna 2009.

[10] Dragana Petrović, Mioslav Lazić, The remote control of power supplies – experiens of exploatation, Serbian journal of electrical engineering, Volume 9, No. 1, February 2012, 95-105, ISSN 1451-4869, UDK:621.311.68-52, DOI:10.2298/SJEE1201095P.

[11] Dragana Petrović, Miroslav Lazić, Dragan Stajić: The remote control of power supplies SDNU aplication for tracking of enviroment quality, 16th Proc. Of the 16th Conf. Power electronics, ISBN 86-7892-208-4, T4-2.9, Novi Sad, okt.26-28, 2011, pp.1-4.

ABSTRACT

The reform of the European Union legal framework for electronic communications, adopted in 2009, examines the security and integrity of public electronic communications networks and services, and states that providers of public communications services must apply safeguards that guarantee the security and integrity of their networks. Power electronics devices are an integral element of every facility used for the telecommunications and information traffic. In addition, the devices are an integral part of every industrial process. Power electronics devices provide the operation of many different devices and together with them, make the system. Systems can be directly supervised by maintenance sector, but can be significantly far from the sectors that control the operation of the system. For remote systems, it is necessary to organize remote monitoring and management.

REMOTE CONTROL AND DERIVED ALARMS - ROAD TO SMART NETWORKS AND ANSWER TO EUROPEAN RECOMMENDATIONS

Bojana Jovanović, Dragana Petrović, Miroslav Lazić, Branko Blanuša