TEHNIČKO REŠENJE BITNO POBOLJŠAN POSTOJEĆI PROIZVOD

Bitno poboljšan postojeći proizvod: NOVI SOFTVER U SISTEMU ZA DALJINSKI NADZOR I UPRAVLJANJE-SDNU ZA SNMP

Rukovodilac projekta: Miloš Živanov
Odgovorno lice: Dragana Petrović
Autori: Dragana Petrović, Miroslav Lazić, Bojana Jovanović, Zoran Cvejić, Miroslav Ilić

Razvijeno: U okviru projekta III43008
Godina: 2012.
Primena: 01.06.2012.

Kratak opis

SNMP (*Simple Network Management Protocol*) je široko rasprostranjen protokol za nadzor i upravljanje uređajima koji se nalaze na računarskim mrežama.

Sistem za daljinski nadzor i upravljanje SDNU prestavlja sistem za praćenje i upravljanje radom uređaja energetske elektronike. Sva prikupljena merenja i alarmi prenose se do udaljenog centra za nadzor u lokalnom formatu sistema SDNU. Ukoliko se pojavi potreba za prosleđivanjem poruka ka višem hijerahijskom nivou ili ka glavnom centru za nadzor poruke se mogu prepakovati u SNMP format i poslati na željenu adresu. Svaka SNMP poruka mora da sadrži set neophodnih informacija kao što su identifikacioni broj, lokacija i uređaj koji je inicirao slanje poruke, vreme kada je poruka (alarm) nastao, prioritet alarma i stanje alarma.

Tehničke mogućnosti

Omogućen je nadzor različitih tipova uređaja i različitih proizvođača.
Softver omogućava prenos podataka po unapred definisanom protokolu (SNMP)
Omogućeno je praćenje rada uređaja energetske elektronike zajedno sa ostalim sistemima
Olakšano je praćenje rada uređaja energetske elektronike
Omogućeno je klasifikovanje alarma

Realizatori

Institut za telekomunikacije i elektroniku IRITEL a.d. Beograd

Korisnici

Iritel a.d. Beograd – proizvođač, Telekom Srbija a.d, Telekom Srpske a.d, Elektrodistribucija Beograd i ostale kompanije koje imaju oformljen glavni nadzorni centar (NMS - *Network Management System).*

Do kraja 2012 godine novi softver je instaliran u Telekomu Srpske. Pod nadzorom se nalazi 130 perifernih uređaja i u Telekomu Srbija pod nadzorom se nalazi 90 perifernih uređaja.

Stanje u svetu

Zadatak u održavanju široko rasprostranjene računarske mreže je da se održe u funkciji vitalni resursi kao što su ruteri, svičevi, serveri i svi ostali elementi neophodni za nesmetan rad mreže. Istovremeno, postoji više razloga zbog kojih je poslovnim sistemima važan nadzor uređaja: ostvareni protok, problemi sa kablovima ili pojedini parametri uređaja. Praćenje rada mreže i uređaja istovremeno je i dobar početak u otkrivanju sigurnosnih problema.
SNMP je standardni i vrlo raširen protokol za upravljanje i administraciju mreže koji služi za prikupljanje informacija o subjektima na mreži i njihovo slanje administratoru. SNMP se naslanja na UDP (*User Datagram Protocol*).
SNMP (*Simple Network Management Protocol*) je nastao 80-tih godina sa ciljem da jednostavno integriše upravljanje heterogenim mrežam. Zasnovan je da radi na aplikativnom nivou koristeći TCP/IP kao transportni protokol i time ne zavisi od mrežnog hardvera. Svaki uređaj u sebi sadrži hardverski i softverski deo prilagođen prenosu podataka po unapred usaglašenom protokolu. Omogućen je nadzor različitih tipova uređaja i različitih proizvođača. SNMP je evoluirao od verzije v1, preko v2c do v3 u kojoj je zaštita podataka podignuta na viši nivo.
SNMP je veoma jednostavan protokol. Predviđene su samo dve operacije, a to su upit i zadavanje vrednosti neke promenljive. Proširenje protokola je u direktnoj zavisnosti od toga kako se definiše baza (MIB - *Management Information Base*).
SNMP arhitektura se sastoji od dva ključna elementa: agenta i menadžera. Radi se o klijent-server arhitekturi u kojoj je agent server, a menadžer klijent.
Agent je program koji se izvršava na svakom upravljivom ili nadziranom čvoru mreže i obezbeđuje interfejs ka svim opcijama konfiguracije. Ove opcije se čuvaju u MIB bazi. Agent ima lokalno znanje o upravljačkim informacijama i prevodi ih u oblik kompatibilan sa SNMP. Omogućava udaljeni pristup opremi za upravljanje.
Menadžer je softver koji se izvršava na nadzornoj stanici mreže. Uloga menadžera je da kontaktira razne agente i periodično prozove i prikupi podatke. To je klijent strana pri nadzoru i upravljanju.

Opis sistema

Glavni nadzorni centri (NMS - *Network Management System*) namenjeni su za praćenje rada različitih sistema i uređaja. Zbog toga, u centar stiže značajan broj poruka o stanju posmatranog sistema. Centri za nadzor obično su namenjeni praćenju rada različitih sistema i uređaja tako da postoji mogućnost da se za kratko vreme pojavi veliki broj informacija. Neki od alarma koji se generišu i prosleđuju centru za nadzor mogu se predvideti i zanemariti sobzirom na količinu informacija koja se „sliva“ u centar za nadzor. Da bi se izbeglo „zatrpavanje“ alarmima, set podataka koji se prosleđuje u centar za nadzor od svakog uređaja svodi se na minimum. Taj set podataka je nedovoljan za detaljnu analizu rada uređaja, ali je svakako dovoljan za praćenje trenutnog stanja sistema. Bitne informacije za glavni nadzorni centar vezane su za stanje sistema kada postoji mogućnost otkaza kao i informacije da se desio otkaz nekog dela ili kompletnog posmatranog sistema.

Da bi pristigle poruke bile uočljive i da bi se akcenat stavio na alarme koji su bitni za određeni periferni objekat ili sistem pristupa se SNMP formatu prenosa podataka. SNMP (*Simple Network Management Protocol*) je nastao sa ciljem da jednostavno integriše upravljanje heterogenim mrežam. Omogućen je nadzor različitih tipova uređaja i različitih proizvođača. Na ovaj način poruke se primaju sa unapred definisanim informacijama tako da dispečeru ne treba mnogo vremena da dešifruje poruku i primljeni alarm.

Zbog velikog broja informacija, SDNU svoje podatke prosleđuje ka centru za nadzor namenjen isključivo jednom tipu opreme-konkretno uređaji energetske elektronike se posmatraju u centru za nadzor napajanja. Na ovom mestu, nazvan Ekspertski centar mogu se videti izmerene veličine svih uređaja i sistema iz posmatranih objekata. Alarmi, incidenti,

izveštaji i dijagrami veoma su bitni službama održavanja radi jednostavnijeg funkcionisanja. Detaljne informacije koje prikuplja SDNU, svakako su potrebne i ne sme se dozvoliti da se bilo koja informacija „izgubi“. Službe održavanja koje su u stalnom kontaktu sa posmatranom opremom moraju imati sve informacije kako bi kvalitetno analizirale rad sistema i odreagovale u pravom trenutku. Informacija koju korisnik dobije u momentu kada je došlo do kvara je zakasnela informacija. Poruke o stanju sistema koje ukazuju na to da će doći do otkaza su „prave“ poruke koje u pravom trenutku treba da stignu do pravog čoveka.

Da bi službe održavanja imale sve potrebne informacije o stanju posmatranih uređaja i sistema, a glavni nadzorni centar neophodne alarme, SDNU je unapredio softver tako da se izabrane poruke prenose i ka glavnom nadzornom centru.

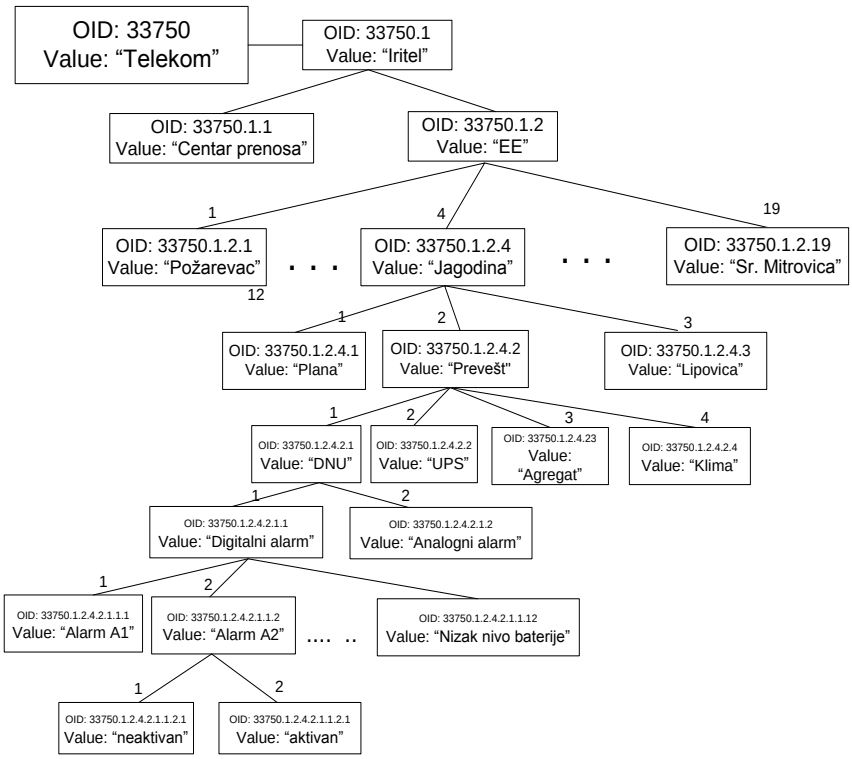
Pri prenosu informacija u SDNU posebna pažnja posvećena je sledećem:

- da svi podaci budu prosleđeni odgovarajućim službama,
- da se slanje poruke dogodi istog trenutka kada je podatak zatražen od strane službi održavanja
- da se informacija automatski prosleđuje u slučaju pojave incidentne situacije (alarma),
- da se pošalje detaljno snimljen dijagram incidentne situacije,
- da se da se spreči gubitak podataka,
- da se ponovo pošalje svaka poruka koja nije stigla u očekivanom formatu ili sa očekivanim brojem bajtova,
- da se informacije čuvaju dok se ne prosledi i ne dobije povratna poruka o pravilno primljenoj informaciji,
- da se što manje opterećuje prenostni put.

Specifičnost SDNU zasniva se na pakovanju poruka za slanje. Ako poruka sadrži veliki broj bajtova povećava se verovatnoća da neće biti dobro prenešena. Iz tog razloga poruke se pakuju u blokove označene stranicom i brojem bloka. U slučaju da dođe do greške u prenosu ponovo se šalje samo potreban blok. Na ovaj način realizovana je maksimalna ušteda vremena i zauzetosti prenosnog puta.

Da bi se SDNU vezao za glavni korisnički centar za akviziciju podataka (NMS) poruke se prepakuju u format definisan za SNMPv2c. Prvenstvano se određuje MIB baza koja prikazuje kako će biti definisani čvorovi u sistemu. Na slici 1 slikovito je prikazana MIB baza koja je predstavljala osnovu u povezivanju uređaja na glavni nadzorni centar. MIB baza vezana je samo za alarme u sistemu SDNU.

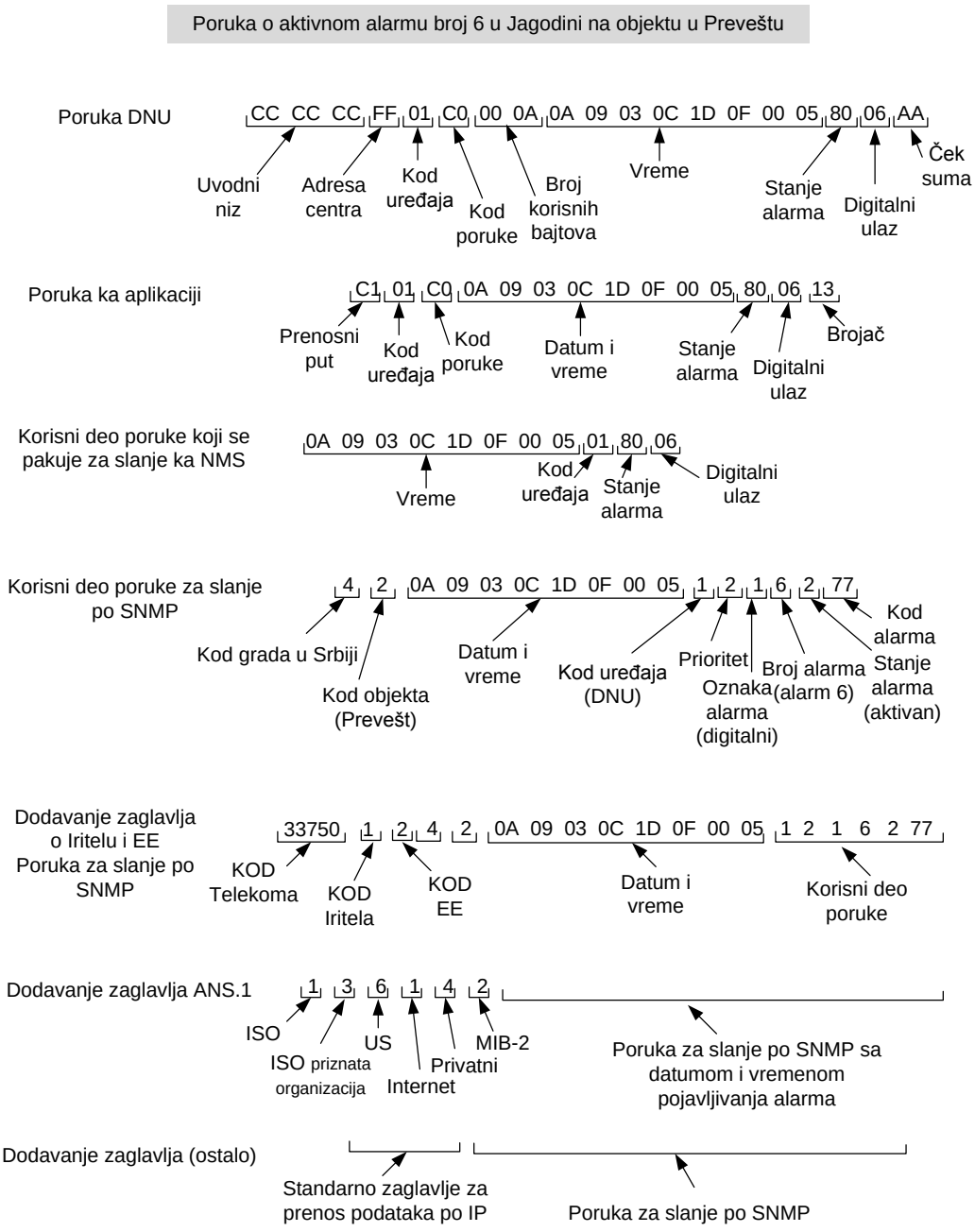
Sa slike 1 se jasno vidi da grad u Srbiji predstavlja jedan MIB objekat (čvor) označen svojim ID brojem (identifikacioni broj) i vrednosti. Nakon toga tabela se grana u čvorove koji predstavljaju periferne objekte, zatim uređaje energetske elektronike. Nakon toga dolazi se do objekata koji predstavljaju vrste alarma. Na kraju je definisan status alarma - aktivan ili neaktivan.



Slika 1: MIB tabela u SDNU

Na slici 2 prikazani su koraci kodiranja poruke, od poruke koja se formira nakon aktiviranja alarma u DNU 24 do poruke koja se šalje ka glavnom nadzornom centru (NMS - Network Management System). Primer je prikazan aktiviranjem digitalnog alarma broj 6 u Jagorini na objektu u Preveštu. Poruka forimirana za slanje po SNMP sadrži sve potrebne elemente tako da je korisniku nedvosmisleno jasno koji alarm se desio na kom perifernom objektu.

Svaka poruka u DNU24 pored informacije o alarmu nosi i informacije o uređaju na kojem se desio alarm. Ta poruka se dalje prepakuje u format koji nosi informaciju o prenosnom putu. U slučaju slanja po SNMP korisni deo poruke se koduje tako da odgovara karakteristikama SNMP i napred definisanoj MIB tabeli. Nakon toga, postavljaju se ID brojevi i vrednosti na čvorove koji su uobičajeni za slanje Iritelove opreme energetske elektronike u preduzeću Telekom Srbija. Dodavanje zaglavlja vezano za ANS.1 vrši se automatski kao i standardni okviri za IP.



Slika 2: Kodovanje poruke SDNU u SNMP

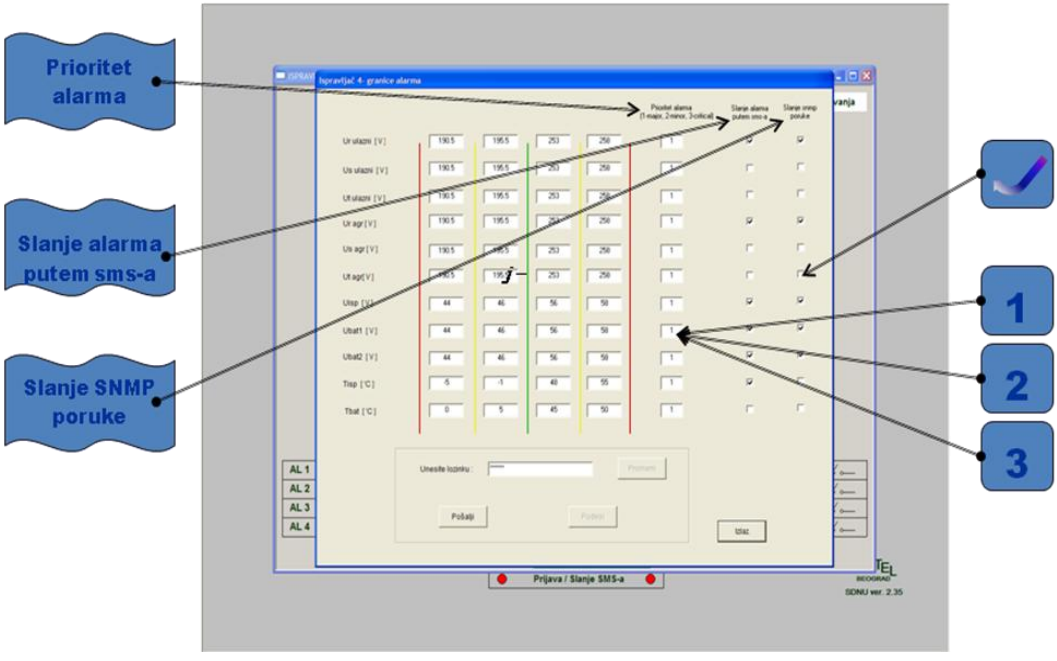
Korisni deo poruke koja se prepakuje u SNMP format i šalje ka glavnom nadzornom centru sastoji se od koda uređaja, vremena kada se alarm dogodio, stanje alarma i digitalni ulaz. Digitalni ulaz označava naziv alarma koji se aktivirao. Ovi podaci su dovoljni da dispečer može da zaključi o kom alarmu je reč i da odreaguje u skladu sa priloženim uputstvom. Međutim kada u glavni centar stigne veliki broj sličnih poruka, javlja se mogućnost da se neki previde. Zbog toga je korisnom delu poruke dodato nekoliko neophonih podataka i u skladu sa tim modifikovana prikazana MIB baza.

Jedan od dodatih podataka je prioritet alarma. Svakoj vrsti alarma dodeljuje se određeni prioritet: slabi, srednji, ili kritični (*minor*, *megor* ili *critical*). U skladu sa poslatim kodom o prioritetu alarma, u glavnom centru za nadzor može se priključiti određena boja ili neki drugi vid raspoznavanja kritične poruke. Koja poruka je kritična i kako odrediti njen prioritet može da se oceni samo na osnovu izmerenih veličina i stanja sistema u posmatranom objektu. Službe održavanja najbolje poznaju uređaje za koje su zaduženi i zato bi bilo najbolje da se na tom

mestu i određuje prioritet. Nisu svi objekti istog značaja pa stoga ni pojedini alarmi nemaju isti prioritet.

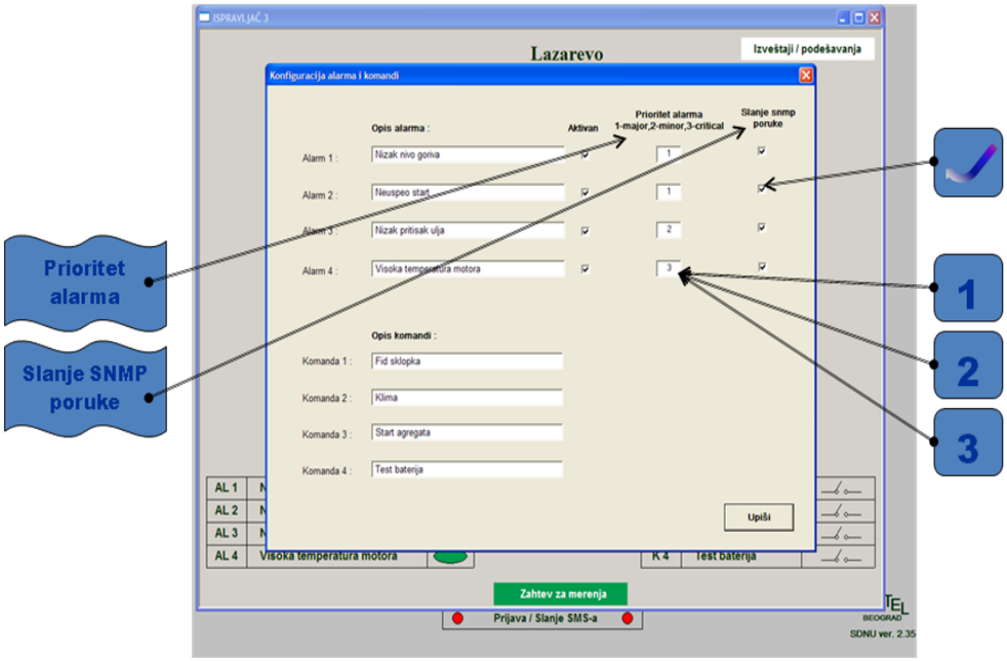
Drugi bitan podatak je kodni broj, odnosno *kod* aktivnog / neaktivnog alarma koji se razlikuje za svaki poslati alarm. *Kod* alarma se dodeljuje onog momenta kada se alarm aktivira. Onog momenta kada alarm postane neaktivan, odnosno izmerena veličina se vratila u regularan opseg rada u glavni nadzorni centar se šalje poruka sa istim *kodom* kao i poruka o aktiviranju alarma. Na opisan način u glavnom dispečerskom centru se poništavaju sve poruke (alarmi) koji su neaktivni i time se smanjuje broj alarma prikazanih na monitoru. Ukoliko ovaj podatak ne bi postojao, u glavnom nadzornom centru bi bilo mnogo teže da se povežu aktiviran i deaktiviran alarm. Sa postojanjem *koda* poruke, gotovo automatski deaktivirani alarmi se sklanjaju sa aktivnog „prozora" i smeštaju u bazu podataka. Baza podataka je organizovana, pregledna i mnogo je jednostavnije dobiti izveštaj za određeni nadzirani uređaj ili željeni alarm. Baza podataka služi za skladištenje podataka tako da korisnik u svakom momentu može da dobije željenu informaciju o alarmima koji su prethodili nekom događaju. Druga značajna uloga baze podataka je da može da se koristi za analiziranje stanja nekog posmatranog objekta, kontrolišući svaki nadzirani uređaj koji se nalazi u objektu.

Na slikama 3 i 4 prikazane su grafičke aplikacije u centru za nadzor na kojima se vrši izbor i podešavanje slanja alarma ka glavnom nadzornom centru. Za svaku izmerenu veličinu vrši se izbor da li da se odstupanje od regularnih vrednosti prenosi kao alarmno stanje ili ne i ukoliko se šalje, koji je prioritet tog alarma. Na slici 3 prikazan je grafički prikaz u centru za nadzor gde se određuju granice merenja analognih veličina. Svaka veličina je ograničena sa dve donje i dve gornje granice. Pored graničnih vrednosti na istom mestu određuje se da li alarmno stanje treba da se šalje ka višem hijerarhijskom nivou (ekspertskom i glavnom nadzornom centru), da li da se šalje sms poruka na unapred dofinisan telefonski broj i koji je prioritet aktivnog alarma. Sve ove parametre upisuje korisnik u centru za nadzor koji je zadužen za održavanje urežaja energetske elektronike u posmatranom objektu. Ukoliko postoji nedoumica u vezi podešavanja, stručnjaci iz ekspertskog centra imaju pristup svakom centru za nadzor i mogu menjati podešene veličine. Prioritet alarma označava se sa 1, 2 ili 3 što znači *minor*, *mesure* ili *critical*. Slanje sms ili SNMP poruke se određuje jednostavnom čekiranjem označenog polja. SNMP poruka će biti poslata ka glavnom nadzornom centru samo ako je čekirana.



Slika 3: Podešavanje slanja analognih alarma

Na slici 4 prikazan je spisak digitalnih alarma i grafička aplikacija na kojoj se bira da li će aktivirani alarm da se prosleđuje ka glavnom nadzornom centru i koji je prioritet alarma. Digitalni alarmi imaju podjednaku važnost kao i analogni i na isti način se i definiše njihovo slanje ka glavnom nadzrnom centru. Postoji mogućnost da digitalni alarm nije povezan na perifernom objektu, tada naziv alarma ostaje prazan i automatski se isključuje mogućnost da se čekira slanje SNMP poruke. Na ovaj način je sprečena mogućnost slučajnog aktiviranja neaktivnog alarma i njegovo slanje ka višem hijerarhijskom nivou.



Slika 4: Podešavanje slanja digitalnih alarma

Kataloški podaci

Primena:
Iritel a.d. Beograd – proizvođač, Telekom Srbija a.d, Telekom Srpske a.d, Elektrodistribucija Beograd i ostale kompanije koje imaju oformljen glavni nadzorni centar (NMS - *Network Management System).*

Novi softver u sistemu za daljinski nadzor i upravljanje-SDNU za SNMP je razvijen od strane Iritel a.d. Beograd, u okviru projekta III43008:" Razvoj metoda, senzora I sistema za praćenje kvaliteta vode, vazduha I zemljišta"

Štampano – Decembar 2012.