DOI: 10.7251/JEPM2201020s
UDC: 004.72.057.4:621.311.42(497.6)

Journal of
Engineering & Processing Management

STRUČNI RAD

SIGURNOST UPRAVLJANJA SCADA SISTEMOM U TRAFOSTANICAMA BIH

Goran Savić[1] | **Goran Tadić**[1]

[1]Univerzitet u Istočnom Sarajevu, Tehnološki fakultet Zvornik, 75400 Zvornik, Bosna i Hercegovina.

Correspondence
Goran Savić, Univerzitet u Istočnom Sarajevu, Tehnološki fakultet Zvornik, 75400 Zvornik, Bosna i Hercegovina
Email: ts.zvornik@gmail.com

Abstract

Rad opisuje koncept savremenih sistema daljinskog nadzora i upravljanja (SCADA) u trafostanicama BiH i uvezivanje u daljinske centre upravljanja sa posebnim osvrtom na aspekt redundancije, pouzdanosti i dostupnosti. Također, bitni aspekti koji su obrađeni u ovom radu su prednosti koje donosi: redundancija RTU-a ili staničnog kontrolera, korištenje redundantnih protokola, korištenje industrijske opreme predviđene za radu elektroenergeskom okruženju te parametrima koje treba zadovoljavati ista. Pored SCADA sistema dat je i osvrt na načine povezivanja opreme unutar trafostanice sa daljinskim centrima upravljanja te osnovnim elementima i zahtjevima na telekomunikacionu opremu.

Keywords: SCADA, redundancija, pouzdanost, dostupnost, sigurnost

1. UVOD

Industrijski sistemi daljinskog upravljanja predstavljaju pravac razvoja i modernizacije velikih industrijskih pogona sa ciljem višeparametarskog nadzora i upravljanja industrijskih ciklusa i kao takvi danas su od vitalnog značaja za funkcionisanje industrijskih sektora na kojima se zasniva kritična infrastruktura države. SCADA (*eng. Supervisory Control and Data Acquisition*) sistemi nadziru i upravljaju u realnom vremenu procesnom opremom smještenom na većem broju geografski distribuiranih lokacija, kada je centralizovano prikupljanje i upravljanje podacima od suštinskog značaja za funkcionisanje procesa. Oni su u širokoj upotrebi u industrijskom sektoru, prvenstveno u proizvodnji, prenosu i distribuciji električne energije, industriji nafte i gasa, vodoprivredi, kao i u saobraćaju i transportu. Otkazi i neispravan rad takvih sistema mogu prouzrokovati ozbiljne posledice zbog njihovog strateškog značaja za kritičnu infrastrukturu svake države. Pouzdanost napajanja električnom energijom je jedan od ključnih zahtjeva za prenosne i distributivne mreže. Sve veće potrebe za električnom energijom dovode i do kontinuiranog razvoja modernih sistema zaštite i upravljanja kao procesa neophodnog za zadovoljavanje pouzdanosti i sigurnosti elektroenergetskih sistema. Koncept modernih sistema zaštite i upravljanja obuhvata širok aspekt tehnoloških dostignuća potrebnih za integraciju svih cjelina EE (skr. elektroenergetskih) postrojenja u jedan kompaktan i pouzdan sistem koji će pored osnovne funkcije sigurnog i pouzdanog rada u periodu eksploatacije, zadovoljavati i ostale elemente definisane standardima i zakonskim normama (Selimić et al. 2014).

Prvi korak u implementiranju savremenih sistema zaštite i upravljanja čini automatizacija EE postrojenja, koja prati opšti tehnološki razvoj komukacionih tehnologija i računarskih sistema, što je rezultiralo korišćenje SCADA sistema koji predstavlja programsku podršku za nadzor i upravljanje energetskim i industrijskim procesima, sa tendencijom ka unrapredjivanju softverskih i komunikacionih mogućnosti, i predstavlja sistem za prikupljanje podataka i funkcija daljinskog nadzora i upravljanja.

Sve do nedavno, komunikacioni i informacioni sistemi su bili periferni i smatrani su od manje važnosti u odnosu na primarnu opremu. U elektroenergetici, fokus je stavljen ekskluzivno na korištenje opreme koja daje pouzdan rad sistema. Međutim razvojem tehnologije, ovi sistemi su postali kritična tačka pouzdanosti. Tako da je danas pored elektroenergetske infrastrukture, informaciona infrastruktura jednako važna stavka u funkcionisanju EE sistema, te se pouzdanost

kompletnog sistema ne može posmatrati odvojeno već kao jedna cijelina.

Informacije predstavljaju najosjetljiviju imovinu, kako u elektroenergetskim kompanijama, tako i u svim ostalim privredama, pa se zbog toga posvećuje velika pažnja njihovoj zaštiti. Računarski podaci, marketinške strategije, porezi, lični zapisi, vojne strategije, finansijski podaci i poslovni planovi su samo neki od niza pojmova koji se kriju iza riječi informacija. Upravo iz tih razloga se razvojem računarskih sistema razvija i informacijska sigurnost. U elektroenergetskim kompanijama se posebna pažnja posvećuje kako zaštiti informacija tako i pristupu sistemima upravljanja.

Pojmovi pouzdanosti, dostupnosti i sigurnosti su od velike važnosti za ovakve sisteme te je potrebno dati poseban osvrt na iste s obzirom na važnost transformatorskih stanica u elektroprenosnoj mreži BiH, pa i uopšte. U ovom radu su opisane dostupne tehnologije, filozofije dizajna SCADA sistema te dobra inžinjerska praksa sve s ciljem povećanja pouzdanosti, dostupnosti i sigurnosti elektroenergetskog sistema.

2. SIGURNOST, DOSTUPNOST, POUZDANOST SCADA SISTEMA

Elemente nacionalne infrastrukture predstavljaju i trafostanice, koje su kritične, i kao takve podložne fizičkim ili virtuelnim prijetnjama koje mogu ugroziti integritet iste. Sigurnosne prijetnje uključuju nehotične opasnosti (kvarovi opreme, prirodne nepogode, ljudska nepažnja) i namjerne opasnosti (virusi i malware, vandalizam, cyber prijetnje, terorizam).

Korištenjem opreme i sistema usklađenih sa međunarodnim standardima je jedini način sprečavanja neželjenih događaja. U SCADA sistemima, u trafostanicama, konstantne promjene i update-i nisu preporučljivi te je potrebno pažljivo planirati redovna poboljšanja sistema. Karakteristike SCADA sistema su:

- Integritet podataka je od krucijalne važnosti,
- Životni vijek opreme do 20 godina,
- Sigurnosni testovi / audit se obavlja rijetko za sistem u pogonu,
- Primjena patch-eva samo u karakterističnim slučajevima,
- Dostupnost / pouzdanost, besprekidan rad sistema bez ispada i kvarova.

Kako bi sistem zadovoljio sve pretpostavljene i neophodne zahtjeve za rad potrebno je uočiti i primjeniti sljedeće preporuke:

- Uređaji, hardware i software:
  - Početne (*eng. default*) postavke svih uređaja bi trebale da imaju onemogućen pristup preko neiskorištenih portova (npr. udaljeni pristup),
  - *Penetration* test za sve nove uređaje na tržištu,
  - Kontinuirana procjena sigurnosti i rizika na sistem,
  - Sigurna autentikacija korisnika kriptovanom konekcijom između uređaja i inžinjerskih alata,
  - Korištenje *WhiteList* filtera za IEC 60870-5-101/104, što podrazumjeva listu dozvoljenih radnji i skup pravila za pojedine konekcije pri čemu je dozvoljeno samo ono što je definisano predmetnim filterima,
  - End-to-Site security, na relaciji kontrolni centar – trafostanica (npr. VPN),
  - End-to-End security, što podrazumjeva enkripciju komunikacije između dva uređaja (npr. application encryption IEC 62351 / TLS).

- Sistem:

- Daljinski centri upravljanja i trafostance povezati sigurnom mrežom (VPN) te procesna mreža i duge mreže odvojene firewall-om, što predstavlja jednostavno rješenje za zaštićeni sistem unutar WAN-a,

- Application layer firewall,
- Ljudski faktor:

- Sigurnosni know-how za osoblje koji imaju bilo kakvog kontakta sa SCADA sistemom,
- Kontinuirano osposobljavanje osoblja za ispravno i sigurno korištenje sistema.

2.1. Međunarodni standardi

Predmetna problematika je tretirana od strane više međunarodnih instituta i tijela za standardizaciju pa tako postoje kontinuirani napori za unapređenja u ovoj oblasti. U nastavku je dat pregled nekih od relevantnih IEC standarda koji bi trebali biti primjenjeni u savremenim SCADA sistemima pa tako i u elektroprenosnom sistemu BiH.

IEC 27001 (*eng. Information Security Management System (ISMS)*) je na međunarodnom nivou sve prihvaćenija norma koja daje preporuke za uspješnu implementaciju efikasnog sistema upravljanja. Razlog prihvaćenosti ovog standarda jest što osigurava fleksibilnost, definiše upravljački okvir, a ne zadire u konkretnu tehničku implementaciju, što ga čini primjenjivim u različitim organizacijama. Ovaj standard opisuje proces uvođenja sistema upravljanja sigurnošću informacija uz očuvanje povjerljivosti, integriteta i raspoloživosti.

Model koji je primjenjen u osnovi ovog standarda je PDCA (*eng. Plan-Do-Check-Act*), naveden kroz svoje dijelove 4-10, što podrazumjeva, (ISO/IEC 2013):

- Plan (uspostaviti ISMS): politiku, ciljeve, procese i procedure važne za upravljanje rizikom i povećanje informacijske sigurnosti, (*poglavlje: 4 Context of the organization, 5 Leadership, 6 Planning, 7 Support*),
- Do (implementirati i izvršavati ISMS): Implementirati i izvršavati ISMS politiku, kontrole, procese i procedure, (*poglavlje 8 Operations*),
- Check (nadgledati i provjeravati ISMS): Procijeniti i, gdje je primjenjivo, mjeriti performanse procesa u odnosu na ISMS politiku, ciljeve i praktično iskustvo te izvještavati upravu o rezultatima, (*poglavlje 9 Performance evaluation*),
- Act (održavati i poboljšavati ISMS): Poduzeti korektivne i preventivne mjere zasnovane na rezultatima internog ISMS nadzora (*eng. audit*) i provjere uprave, kako bi se omogućilo stalno poboljšanje ISMS-a, (*poglavlje 10 Improvment*).

IEC TC57 je jedan od tehničkih komiteta IEC (*eng. International Electrotechnical Commission*) koji je odgovoran za razvoj standarda razmjene informacija između elektroenergetskih sistema i drugih povezanih sistema kao što su Energy Management Systems, SCADA, teleprotection i slično. TC 57 se sastoji od nekoliko radnih grupa gdje su svako od njih zadužena za razvoj standarda unutar svoje domene. U nastavku je dat prikaz nekih značajnijih sa nazivima u orginalu uz prikaz razvijenog IEC standarda:

- Radna grupa 3: Telecontrol & Teleprotection standardi, **IEC 60870-5**,
  - Fokus na razvoju komunikacionih protokola za RTU (*eng. Remote Terminal Unit*) uređaje. Definisan je veliki broj uređaja i podatkovnih modela kako bi se omogućila interoperabilnost za veliki broj uređaja i primjena u elektroenergetskim objektima. Korištenje manjih 8-bitnih brojeva za predstavljanje objekata i informacija maksimizira broj informacija koje je moguće poslati unutar jednog 60870-5 podatkovong okvira. Razvojem mreža i komunikacionih protokola je dovelo do korištenja TCP/IP protokol te razmjena informacija kroz WAN (*eng. Wide Area Network*) mreže.
- Radna grupa 7: Telecontrol protocols compatible with ISO Standards and ITU-T recommendations, **IEC 60870-6 ICCP/TASE.2**
  - Fokus na razvoju sistema razmjene podataka preko WAN-a između kontrolnog nadzornog centra i drugih kontrolnih centara te elektroenergetskih objekata.
- Radna grupa 10: Power system IED communication and associated data models, **IEC 61850**,
  - Fokus na razvoju standarda za automatizaciju unutar elektroenergetskih objekata čije mogućnosti premašuju uobičajne point-to-point protokol rješenja. Neke od većih inovacija koje je ovaj standard donio su razvoj standardiziranog SCL (*eng. Substation Configuration Language*) jezika, i standardizirani funkcijski-orjentisani objekti.
- Radna grupa 13: Energy management system application program interface, **IEC 61970**,
  - Fokus na razvoju interoperabilnosti između kontrolnih centara što uključuje:
  - Energy, Distribution i Outage Management,
  - Geographic Information systems GIS,
  - Network Analysis Applications,
  - SCADA.
- Radna grupa 15: Data and communication security, **IEC 62351**,
  - Fokus na sigurnosnoj analizi i ekspertizi za druge IEC TC57 radne grupe. Ovim standardom su date preporuke za ostvarivanje sigurne application-to-application razmjeni informacija te su obuhvaćeni:
  - Udaljeni nadzorni centri,
  - Trafostanice,
  - Proizvodna postrojenja,
  - Distributivna postrojenja.

Komunikacioni protokoli koji su obuhvaćeni ovim standardom su:

- IEC 60870-5 i sve njegove izvedenice (101, 103, 104, DNP),
- IEC 60870-6 TASE.2, ICCP,
- IEC 61850.

Radna grupa analizira različite prenosne medije i komunikacione putanje kako bi se standardizirala sigurna infrastruktura koja je nezavisna od protokola, ali u isto vrijeme i sposobna za detektovanje upada i napada na sistem.

- Radna grupa 16: Deregulated energy market communications, **IEC 62325**,
  - Fokus na razvoj standarda vezanih za tržištu električne energije što uključuje dobavljače, potrošače, trgovce i menadžere.
- Radna grupa 19: Interoperability within TC 57 in the long term, CIM i SCL vezani standardi.

  - Fokus na cijelovitom prikazu svih dijelova sistema (standardi i druge radne grupe) kojim se može steći globalna slika stanja sistema te mogući sveukupnu uticaji na sistem u cjelini uzrokovani nekom promjenom bez potrebe za detaljnim znanjem rada pojedinačnih uređaja i elemenata sistema. Najveći benefit je mogućnost izmjene individualnih uređaja i aplikaciji razvojem novih sistema uz male ili nikakve uticaje na sistem u cjelini što daje kao rezultat veću pouzdanost uz manje troškove.

Svi standardi koji su nastali iz radnih grupa dijele zajedničku strukturu tzv. model-orjentisanu arhitekturu koja definiše standard na tehnološki neutralan način tj. odvaja virtuelni model od tehnoloških detalja što omogućava primjenu standarda na postojeće sistema npr. standardizirani nazivi u SCADA sistemu, bez dodavanja nove opreme i instalacije novih sistema. Glavna motivacija za model-orjentisanu arhitekturu je brza promjena i razvoj komunikacionih veza (način interakcije) između dijelova sistema u odnosu na sporiju promjenu standarda vezanih uz npr. primarnu opremu elektroenergetskih objekata.

Jedna od kritičnih aspekata predmentih sistema su komunikacioni protokoli koji posreduju razmjeni informacija i slanju upravljačkih komandi. Uprkos svom značaju, sigurnosne mjere (kvarovi opreme, greške komunikacione opreme, namjerne sabotaže i slično) nisu njihov sastavni dio.

Elektroenergetske mreže predstavljaju privlačne mete za napade što pokazuju napadi na elektroenergetsku distributivnu kompaniju Kyivoblenergo, Ukrajina iz 2015.godine, te napadi na pet indsutrijskih postrojenja nuklearnog programa, Iran – Stuxnet virus te druge malware napade.

Za predmetno pitanje sigurnosti, pouzdanosti i dostupnosti u trafostanicama potrebno je detaljnije dati pregled IEC standarda IEC 62351, (IEC 2007a; 2007b; 2013; 2016a), koji je obuhvatio sljedeće dijelove:

- IEC/TS 62351-3: Security for profiles including TCP/IP,
  - Treći dio standarda obrađuje TCP/IP bazirane komunikacione protokole IEC 60870-5-104, IEC 60870-6 TASE.2, ICCP, IEC 61850. U osnovi koristi TLS (*skr. Transport Layer Security*) koji je uobičajno korišten na Internetu za sigurnu komunikaciju što uključuje autentikaciju, povjerljivost i integritet. Upadi u sistem te zaštite od istih koji su ovim standardom obrađeni su:
    * Zaštita od prisluškivanja TLS enkripcijom,
    * Zaštita od man-in-the-middle sigurnosnog rizika korištenjem autenikacije poruka,
    * Zaštita od spoofing-a korištenjem Security certifikata.

Slabosti ovog standarda su nemogućnost odbrane od DoS napada, te se isti trebaju tretirati drugim mjerama zaštite.

- IEC/TS 62351-4: Security for profiles including MMS,
  - Četvrti dio standarda obezbjeđuje sigurnost za profile koji uključuju Manufacturing Message Specification (skr. MMS) unutar IEC 61850 i to korištenje TLS-a (sigurnosne provjere dvije strane koje razmjenjuju podatke). Dozvoljeno je korištenje secure i non-secure profila kako ne bi bilo potrebno vršiti dogradnju sistema sa sigurnosnim mjerama.

- IEC/TS 62351-5: Security for IEC 60870-5 and derivatives,
  - Peti dio standarda obezbjeđuje različita rješenja za serijske verzije protokola kao i za mrežne.
  - Mrežne verzije komunikacionog protokola IEC 60870-5-104 i DNP 3 zahtjevaju dodatnu autentikaciju prilikom uspostavljanja veze.
  - Serjske verzije komunikacionih protokola IEC 60870-5-101, 103 su namjenjeni i podržavaju niske brzine razmjene podataka pa tako TLS ne dolazi u obzir zbog komunikacijskih zahtijeva na mrežu. Iz tog razloga zaštita od spoofing, modifikacije i DoS napada je omogućena korištenjem autentikacije komunikacije. Međutim, u tom slučaju nije moguće zaštititi sistem od prisluškivanja i analize saobraćaja. Obje ove stavke su važne za sistem, ali mehanizam zaštite u ovim slučajevima je još u toku diskusije.

- IEC/TS 62351-6: Security for IEC 61850 profiles,
  - Šesti dio standarda obrađuje zaštitu GOOSE poruka kao dio standarda IEC 61850. Karakteristika GOOSE poruka koji je dizajniran da prenosi podatke peer-to-peer unutar 4 ms jeste ta da dodatne zaštite bi uzrokovale kašnjenja pa je iz tog razloga kao jedina mjera zaštite autentikacija kako bi poruke bile „digitalno potpisane“.

2.2. Komunikacioni protokoli

U kontekstu sistema zaštite i upravljanja različiti uređaji sistema su komunikaciono povezani i između njih se vrši razmjena informacija. Komunikacija predstavlja razmjenu informacija između izvora i odredišta. Komunikacioni protokol je skup pravila za komunikaciju u mreži. Komunikacioni sistemi predviđeni za korištenje u EE okruženju trebaju zadovoljavati kriterije kao što su: pouzdanost, kvalitet, brzina i sigurnost te su neki od najčešće korištenih međunarodnih industrijskih standarda namjenjeni za upravljanje i automatizaciju postrojenja u elektroenergetskom sistemu (*skr. EES*):

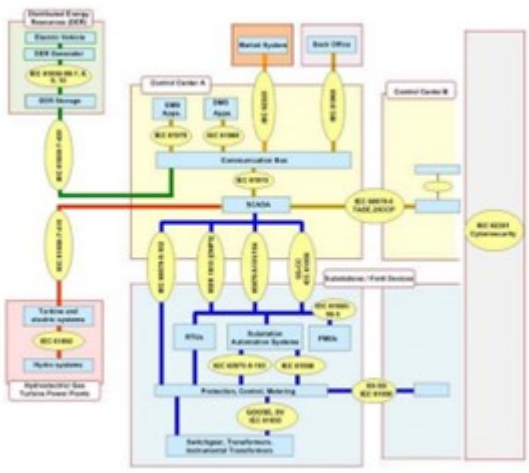
- IEC 60870-5 (IEC 2016b),
  - Skup protokola za komunikaciju između zaštitno-upravljačkih uređaja i za rad sa SCADA sistemom na nivou TS. Komunikacioni protokoli su ostvareni serijskom vezom (IEC 60870-5-101, IEC 60870-5-103) ili TCP/IP vezom (IEC 60870-5-104).
- IEC 60870-6 (ICCP/TASE.2) (IEC 2016a),
  - Komunikacioni protokol za razmjenu informacija između dispečerskih centara te između daljinskih centara upravljanja i elektroenergetskih objekata.
- IEC 61850 (IEC 2016c),
  - Skup protokola sa jasno definisanim pravilima za razmjenu podataka između funkcijskih čvorišta EES-a čime je omogućena interoperabilnost uređaja u sistemu zaštite, nadzora, upravljanja te automatizacija TS nezavisno od proizvođača opreme što je dovelo do unificiranosti i fleksibilnosti u EE postrojenjima.

Od prethodno pobrojanih komunikacionih standarda i protokola, posljednjih godina pri realizaciji koncepta modernog SCADA sistema najčešći i najuobičajeniji su IEC 61850 kao komunikacijski standard za sve uređaje u EE objektima te IEC 60870-5-101 i IEC 60870-5-104 za vezu ka daljinskim centrima upravljanja. Za razliku od prethodnih komunikacijskih standarda koji su bili signal-orjentirani, IEC 61850 je objektno-orjentisan pri čemu je ovim standardom izvršena virtuelizacija, što znači objektni modeli fizičkih uređaja su povezani sa procesnim podacima ključnim za njihov nadzor i upravljanje, (IEC 2016c). Ovim su definisane klase podataka koji sadrže jedinistvenu putanju pojedinog podatka, te su osnovni atributi svakog procesnog podatka: vrijednost, kvalitet i vremenska oznaka. Glavne karakteristike i mogućnosti IEC 61850 komunikacionog standarda i protokola su:

- Korištenje virtuelnog modela,
  - Pored definisanja načina slanja podataka, ovi modeli dozvoljavaju definisanje podataka, servisa i ponašanja uređaja.
- Korištenje opisnih imena za adrese,
  - Svaki element, podatak je imenovan korištenjem opisnog niza karaktera.
- Standardizirana imena objekata,
  - Imena objekata ne definišu ni korisnici ni proizvođači opreme, već su imena definisana standardom.
- Usluge visokog nivoa,
  - Korištenje horizontalne komunikacije (GOOSE), vertikalne (MMS), sample measured value i drugi.
- Jezik SCL (eng. Standardised substation Configuration Language),
  - Korištenjem XML datoteka definisanje uređaja i elemenata.
- Manji troškovi integracije, instalacije te manji infrastrukturni troškovi vezani za ožičenje i kabliranje.

IEC 61850 standard za razliku od drugih komunikacionih protokola definiše model sistema koji je opisan u SCL datoteci za svaku informaciju te se sastoji od:

- Fizičkog uređaja sa IP adresom,
  - fizički uređaj – zaštitno-upravljački uređaj,
- Logičkog uređaja (*eng. logical device*),
  - unutar svakog fizičkog uređaja postoji više logičkih uređaja, konfigurisan slobodno definiran naziv zaštitno-upravljačkog uređaja,
  - Logičkog čvora (*eng. logical nodes*),
  - unutar svakog logičkog uređaja, predefinisana grupa informacija iz softverskog projekta zaštitnoupravljačkog uređaja, gdje postoji 13 različitih grupa i 86 različitih klasa.
- Grupe su sljedeće:
  - sistemske informacije (*eng. System information*),
  - informacija o fizičkom uređaju (*eng. Physical device information*),
  - mjerne veličine (*eng. Measurands*),
  - mjerene vrijednosti (*eng. Metered values*),
  - podaci upravljanja (*eng. Controllable data*),
  - statusne informacije (*eng. Status information*),
  - postavke (*eng. Settings*).



Slika 1. Arhitektura komunikacionog standarda (Cleveland 2012).

- Podaci (*eng. data*), naziv informacija unutar grupe,
- Atribut, atribut same informacije.

Dva dijela IEC 61850 standarda koja su od posebnog značaja za komunikaciono povezivanje i ostvarivanje potrebnih funkcija unutar SCADA sistem su MMS (*eng. Manufacturing Messaging Specification*) za ostvarivanje vertikalne komunikacije u SCADA sistemu (razmjena informacija sa nadređenim sistemima nadzora i upravljanja) te GOOSE za ostvarivanje horizontalne komunikacije sistema (*funkcije blokada - interlocking*). Ovaj standard predstavlja samo središte i nezaobilazan je u implementaciji modernog SCADA sistema.

Na slici 1. je prikazana arhitektura komunikacionog standarda sa korištenim komunikacionim protokolima, prethodno spomenutih u ovom radu, u modernim SCADA sistemima.

3. KONCEPTUALNA ARHITEKTURA SCADA SISTEMA

Kada je reč o realizaciji koncepta modernog SCADA sistema, to bi podrazumjevalo sve neophodne radove, hardversku opremu i softverska rješenja uz uvažavanje ključnih atributa dizajna kao što su: usklađenost sa aktuelnim standardima (svjetski renomirani proizvođači), raspoloživost sistema (99,95%, sa ostvarenom redudancijom svih kritičnih tačaka), mogućnost proširenja (jednostavno proširenje čitavog sistema bez velikih zahvata na istom), skalabilnost (jednostavna i moguća nadogradnja sistema) i otvoren distribuiran dizajn. Bilo da je riječ o izgradnji nove ili rekonstrukciji postojeće TS, SCADA sistem predstavlja nezaobilazan faktor u izgradnji modernog sistema zaštite i upravljanja.

Kako bi se mogli postaviti specifični zahtjevi na sistem, napravljena je podjela trafostanica (IEC 2003) i to:

- Distributivne trafostanice,
  - Naponski nivo 30 kV i niže,
  - Opremljena dominantno odlaznim vodovima,
  - Moguće je da postoje jedan ili dva dolazna voda koji mogu biti sa višeg naponskog nivoa.
- Prenosne trafostanice,
  - Naponski nivo 100 kV i više,
  - Moguće je da ima i dio odlaza nižeg naponskog nivoa.

Ove podjele nisu striktne te mogu biti napravljene i drugačije zavisno od sistema. Također je bitno istaći da tipovi trafostanica i komunikacioni zahtjevi nisu striktno vezani uz veličinu i konfiguraciju trafostanice. Ovaj rad obrađuje trafostanice BiH pa je tako dalja podjela napravljena na sljedeći način:

- T1 mala prenosna trafostanica,
  - Sastoji se obično od manje od 10 elemenata sa mnogo manjom važnošću u elektroenergetskom sistemu,
  - Redundantne zaštite nisu neophodne,
  - Automatizacija se svodi na RTU – gateway i jednostavni HMI.
- T2 velika prenosna trafostanica,
  - Sastoji se od više od 10 elemenata sa važnim mjestom u elektroenergetskom sistemu,
  - Korištenje rezervnih i redundantih zaštita,
  - Lokalni SCADA sistem – HMI u punom obimu,
  - Komunikacija između zaštitno-upravljačkih uređaja se zahtjeva,
  - Opcioni zahtjev za redundanti link unutar trafostanice kao i između trafostanice i udaljenog kontrolnog centra.
- Kombinovana trafostanica (prenosni tip i distributivni tip).

Konceptualna arhitektura modernih staničnih SCADA sistema treba minimalno sadržavati sljedeće elemente:

- Koncentrator podataka – gateway, telemetrijski uređaj (RTU)
- Decentralizovana lokalna mreža – LAN,
- SCADA server,
- operatorsko radno mjesto (HMI preglednik),
- GPS prijemnik sa antenom za vremensku sinhronizaciju uređaja.

3.1. Koncentrator podataka – gateway (RTU)

Koncentrator podataka - gateway uređaj (RTU) predstavlja uređaj za prikupljanje, obradu i proslijeđivanje informacija između nivoa polja, staničnog nivoa i daljinskog centra nadzora i upravljanja. Može se koristiti kao: centralna jedinica sistema daljinskog nadzora i upravljanja ili kao dio istog, front-end jedinica te jedinica za funkcije automatizacije sa autonomnim funkcijskim grupama sa lokalnim ili udaljenim perifernim elementima.

U slučaju velikih prenosnih trafostanica, zbog samog značaja, preporuka je ispunjavanja uslova redundancije sistema i to na sljedeće moguće načine:

- Redundancija napajanja RTU-a,
- Redundancija procesorskih modula i kartica,
- Redundancija kompletnog hardverskog uređaja,
- Redundancija komunikacionog puta sa zaštitno-upravljačkim uređajima.

Tipični zahtjevi za izvedbu RTU-a su sljedeći:

- industrijsko kućište bez pokretnih dijelova,
- konstruisan za neprestan rad sa specificiranim performansama bez smanjenja životnog vijeka,
- sigurnost sistema (zabrana pristupa neovlaštenim osobama),
- mogućnost udaljenog inžinjerskog pristupa,
- mogućnost prihvata i obrade svih informacija po svim uobičajnim komunikacionim protokolima,
- razmjena informacija sa daljinskim centrima upravljanja (gateway funkcija),
- redundantni režim rada hot-standby (napojnih jedinica, procesorskih modula ili kompletnih uređaja), bez gubitka informacija u slučaju kvara na nekom od dijelova RTU ili aktivnom RTU,
- mogućnost izračunavanja vrijednosti izvođenjem aritmetičkih ili logičkih operacija sa real-time podacima (kondicione funkcije, matematičke operacije, relacione funkcije, logičke operacije).

3.2. Decentralizovana lokalna mreža – LAN

Decentralizovana lokalna mreža LAN, SCADA sistema predstavlja skup međusobno povezanih uređaja vezanih za određeni EE objekat. Za prenos informacija, potrebno je koristiti Ethernet komunikacionu infrastruktura, te je prema načinu komunikacionog povezivanja uređaja moguće korisitit jednu od sljedećih uobičajnih mrežnih topologija:

- sabirnička topolgija (zaštitni i upravljački uređaji su direktno povezani na komunikacionu mrežu),
- topologija prsten (zaštitni i upravljački uređaji su međusobno povezani u prsten),
- topologija zvijezda (svaki zaštini i upravljački uređaj je povezan na centralno komunikaciono čvorište),
- topologija višestruka zvijezda (postoji veći broj komunikacionih čvorišta, koji su međusobno povezani u kaskadni niz),
- topologija prsten-zvjezda (zaštini i upravljački uređaji su povezani sa komunikacionim čvorištima korištenjem topologije prsten i zvjezda).

Kako je pouzdanost jedan od najbitnijih faktora, posebna pažnja se treba posvetiti redundantnom radu mreže. Za potrebe automatizacije elektroenergetskih objekata u globalu, razvijen je IEC 62439-3 standard (*Industrial communication networks – High availability automation networks*), (IEC 2012). Dva dijela standarda koja su od posebnog intersa u realizaciji SCADA sistema su:

- IEC 62439-3 clause 4, Parallel Redundancy Protocol – PRP,
  - Svi uređaji su povezani na dvije odvojene LAN mreže istovremeno, te je svaki paket dupliciran na portu i u slučaju ispada porta, dijela jedne mreže ili čitave mreže, druga LAN mreža momentalno preuzima ulogu aktivne LAN mreže.
- IEC 62439-3 clause 5, High-availability Seamless Redundancy – HSR,
  - Svi zaštitno-upravljački uređaji su povezani u topologiji prsten, te šalju multicast okvire preko oba ethernet porta. Na odredištu se prvi primljeni okvir prosljeđuje na dalju obradu, dok se kopija odbacuje.

Glavne karakteristike ova dva dijela standarda su:

- gubitak okvira (eng. Frame loss): nema gubitka okvira,
- uobičajno vrijeme oporavka (eng. Typical Recovery Time): 0 s,
- za identifikaciju pojedinačnih okvira koristi se MAC adresa izvora te broj sekvence.

Glavni zahtjevi pri realizaciji decentralizovane lokalne mreže – LAN za SCADA sistem su sljedeći:

- svi uređaji na nivou polja i na staničnom nivou trebaju biti integrisani u stanični SCADA sistem te komunicirati po lokalnoj mreži LAN,
- jednostavno dodavanje novih čvorova u mreži,
- podržan standard IEEE 802.3,
- ostvarena redundancija na nivou lokalne mreže – LAN,
- korištenje jedne od osnovih topologija mreže, najčešće topologija prsten, zvijeda ili kombinacija ove dvije topologije za složenije mreže sa većim brojem uređaja, čime se postiže redundancija komunikacionog puta.

3.3. SCADA server i operatorsko radno mjesto

SCADA server predstavlja industrijski računar koji ima funkciju nadzora, kontrole i prikupljanja podataka u trafostanici za lokalnu vizualizaciju i obradu podataka te eventualno dodatne gateway funkcije za razmjenu informacija sa daljinskim centrima upravljanja. Zahtjevi koje SCADA server i operatorsko radno mjesto trebaju ispuniti su sljedeći:

- industrijski računar bez pokretnih dijelova i ventilatora predviđen za besprekidan rad,
- mogućnost dodjele različitih korisničkih profila zavisno od autorizacije (operateri, inžinjeri za zaštitne uređaje, sistem inžinjeri)
- displej sa I/O jedinicama za operatorsko radno mjesto,
- vizuelizacija sljedećih preglednih slika:
  - jednopolna shema objekta sa statusima aparata i mjerenim vrijednostima,
  - detaljne jednopolne sheme za svako dalekovodno (skr. DV) i transformatorsko (skr. TR) polje,
  - lista alarma i lista događaja,
- šematski prikaz nadzora rada i komunikacije elemenata sistema,
- mogućnost izrade trendova i izvještaja.

Zavisno od tipa trafostanice, HMI u punom obimu bi uključivao jedan ili dva displeja sa svim detaljima navedenim u tekstu iznad.

3.4. Vremenska sinhronizacija uređaja

Vremenska sinhronizacija u elektroenergetskim objektima predstavlja jako bitan faktor kako bi se tačno mogao utvrditi redoslijed određenih događaja koji se javljaju u periodu korištenja trafostanica. Zahtijev za ostvarivanje vremenske sinhronizacije elemenata SCADA sistema potrebno je ostvariti korištenjem GPS uređaja koji se uobičajno povezuje na lokalnu mrežu – LAN te korištenjem NTP/SNTP komunikacionog protokola vrši vremensku sinhronizaciju elemenata sistema. Ovaj komunikacioni protokol je mrežni protokol koji ima karakteristike vremenske tačnosti od 1 ms u idealnim uslovima u LAN mreži. Mrežna zagušenja mogu izazvati greške od 100 ms i više.

4. SCADA SISTEMI PRIMIJENJENI U ELEKTROPRENOSU SA OSVRTOM NA TRAFOSTANICE U BIH

Predmetni koncept sistema upravljanja (SCADA) je uspješno implementiran u trafostanicama BiH i to u TS 110/35 kV Zvornik, i TS 110/x kV Sarajevo koji je projektovan u skladu sa opštim principima. Ovim projektom je planirana buduća kompletna zamjena SCADA sistem i ugradnja novih uz mogućnost naknadne migracije kompletnog sistema zaštita i upravljanja na IEC 61850 komunikacioni protokol. Ključni atributi dizajna koji su ispunjeni u ovim projektima su:

- Usklađenost sa aktuelnim standardima,
- Visoka raspoloživost sistema sa redudancijom svih kritičnih tačaka sistema (kako na fizičkom tako i na komunikacionim nivou),
- Mogučnost proširenja bez velikih zahvata na istom,
- Otvoren i distribuiran dizajn.

SCADA sistem podrazumjeva korištenje svih trenutno dostupnih tehnoloških rješenja, kako hardverskih tako i softverskih, uz uvažavanje osnovnih principa propisanih međunarodnim standardima i preporukama, pa je ovim projektima implementiran u potpunosti i dimenzionisan za trenutni obim, a i pripravan za eventualna buduća proširenja, za trafostanice ovog tipa.

5. ZAKLJUČAK

Kako su međunarodne institucije i tela za standardizaciju tretitrale problem pomoću IEC standarda za potrebe realizacije modernog sistema daljinskog nadzora i upravljanja (SCADA), tako je ovim stručnim radom dat prikaz rešavanja sigurnosnih pretnji, koji su primjenjivi na trafostanice. Radi lakše i pouzdanije eksploatacije elektroenergetskih visokonaponskih objekata uvodi se moderni sistem daljinskog nadzora i upravljanja, kao jedna od cijelina pri izgradnji nove ili rekonstrukciji postojeće trafostanice, što doprinosi ispunjavanju pomenutih ciljeva.

Glavne prednosti koje donosi ovakav sistem su:

- skalabilnost i otvorenost sistema,
- uvezivanje T u nadležne daljinske SCADA centre,
- pojednostavljen lokalni nadzor i upravljanje,
- unificiranost opreme,
- pouzdan i stabilan rad ostvaren korištenjem opreme renomiranih proizvođača uz ispunjavanje uslova redundantnog režima rada svih komponenti sistema,
- visok stepen raspoloživost i dostupnosti opreme, korištene u distribuiranoj arhitekturi sistema daljinskog nadzora i upravljanja uz uvažavanje međunarodnih normi i standarda.

Standardi su usvojeni skup pravila i tehničkih rješenja određene opreme, uređaja ili sistema, te su proizvod volje i usaglašavanja pod okriljem pojedinih skupina učesnika (proizvođači, operatori, regulatori tijela) sve s ciljem unapređenja i poboljšanja funkcionalnosti. Korištenje preporuka i međunarodnih standarda

doprinose stabilnosti, konstantnom rastu poslovanja sa sve manjim troškovima za korisnike. U ovom radu je dat pregled IEC standarda koje bi trebalo da sistem u cijelini zadovolji i to:

- IEC 27001, za uspostavljanje efikasnog sistema upravljanja,
- IEC 62351, za ostvarivanje sigurne razmjene informacija i sistema,
- IEC 62439, za realizaciju redundantnog LAN-a,
- IEC 61850, skup protokola sa jasno definisanim pravilima za razmjenu podataka između funkcijskih čvorišta EES-a čime je omogućena interoperabilnost uređaja u sistemu zaštite, nadzora, upravljanja te automatizacija TS nezavisno od proizvođača opreme što je dovelo do unificiranosti i fleksibilnosti u EE postrojenjima.
- IEC 60870-5, skup protokola sa velikim brojem uređaja i podatkovnih modela kako bi se omogućila interoperabilnost i primjena u EE objektima.

Također, u radu je dat pregled osnovnih zahtjeva za sve elemente sistema generalno, te uz ispunjavanje prethodno pobrojanih međunarodnih standarda, dat okvir za trafostanice BiH, za uspješnu implementaciju modernog SCADA sistema posebno sa aspekta pouzdanosti, redundantnosti, dostupnosti i sigurnosti.

LITERATURA

Cleveland, F. (2012). Iec tc57 wg15: Iec 62351 security standards for the power system information infrastructure. *White Paper*.

IEC. (2003). *Technical report IEC TR 61850 -1, part 1* (Tech. Rep.).

IEC. (2007a). *62351-6-Power systems management and associated information exchange–Data and communications security–Part 6: Security for IEC 61850*.

IEC. (2007b). *62351-1 Power Systems Management and Associated Information Exchange-Data and Communications Security-Part 1: Communication Network and System Security-Introduction to Security Issues*.

IEC. (2012). *62439-3:2012 Industrial communication networks–High availability automation networks–Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) Réseaux industriels de communication–Réseaux d'automatisme à haute disponibilité–*.

IEC. (2013). *IEC 62351-5 Power systems management and associated information exchange-Data and Communication Security-Part 5: Security for IEC 60870-5 and Derivatives. Draft*.

IEC. (2016a). *IIEC 60870-6, Telecontrol equipment and systems - Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations*.

IEC. (2016b). *IEC 60870-5-SER, Telecontrol equipment and systems - Part 5: Transmission protocols*.

IEC. (2016c). *61850-SER Communication networks and systems in substations*.

ISO/IEC. (2013). *ISO/IEC 27001:2013, Information security management systems*.

Selimić, A., Kalajdžisalihović, E., Cokić, A., Čekić S. Gavrilović, Đuričić, M., & Marić, A. (2014). Modernization of protection and control system of 220 kv switchgear in hpp salakovac, bh. *Electrical Engineering*, *8*, 62–70.

DOI: 10.7251/JEPM2201020s
UDC: 004.72.057.4:621.311.42(497.6)

Journal of
Engineering & Processing Management

PROFESSIONAL PAPER

RELIABILITY OF SCADA SYSTEMS IN BIH SUBSTATIONS

Goran Savić[1] | **Goran Tadić**[1]

[1]University of East Sarajevo, Faculty of Technology Zvornik, 75400 Zvornik, Bosnia and Herzegovina.

Correspondence
Goran Savić, University of East Sarajevo, Faculty of Technology Zvornik, 75400 Zvornik, Bosnia and Herzegovina
Email: ts.zvornik@gmail.com

Abstract

This paper describes the concept of modern SCADA systems in general, as well as in B&H substations, and its connection to remote control centers, with a focus on redundancy, reliability and availability. Also, benefits from the usage of redundant protocols, RTU redundancy, usage of industrial equipment designed to work in substation environment and parameters needed for these systems are discussed in this paper. Besides local SCADA systems, telecommunication issues regarding connection to remote control centers are also considered.

Keywords: SCADA, redundancy, reliability, availability, security