SCADA SISTEMI U CLOUD OKRUŽENJU

Mirjana D. Stojanović[1], Slavica V. Boštjančič Rakas[2], Jasna D. Marković-Petrović[3]
[1]Univerzitet u Beogradu – Saobraćajni fakultet, m.stojanovic@sf.bg.ac.rs
[2]Univerzitet u Beogradu – Institut Mihajlo Pupin, slavica.bostjancic@institutepupin.com
[3]PD "HE Đerdap" – HE "Đerdap 2" Negotin, Jasna.Markovic@djerdap.rs

Sadržaj: *U radu je prvo objašnjen princip funkcionisanja SCADA sistema, a zatim su razmatrane strategije migracije SCADA sistema ka javnoj, privatnoj ili hibridnoj cloud infrastrukturi. Sledi analiza izbora cloud servisa: infrastruktura, platforma ili softver kao servis. Posebna pažnja posvećena je analizi prednosti i rizika pri implementaciji SCADA sistema u cloud okruženju.*

Ključne reči: *Bezbednost, cloud infrastruktura, kvalitet servisa, SCADA.*

1. Uvod

SCADA (*Supervisory Control And Data Acquisition*) sistemi upravljaju u realnom vremenu procesnom opremom smeštenom 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.

Savremeni SCADA sistemi zasnovani su na otvorenim komunikacionim standardima kao što su Eternet, TCP/IP (*Transmission Control Protocol/Internet Protocol*) skup protokola i bežični standardi (IEEE 802.x, *Zigbee*, *Bluetooth*, *WirelessHART*). Tendencija umrežavanja nastavlja se ka okruženjima kao što su *smart grid* i *cloud* računarstvo.

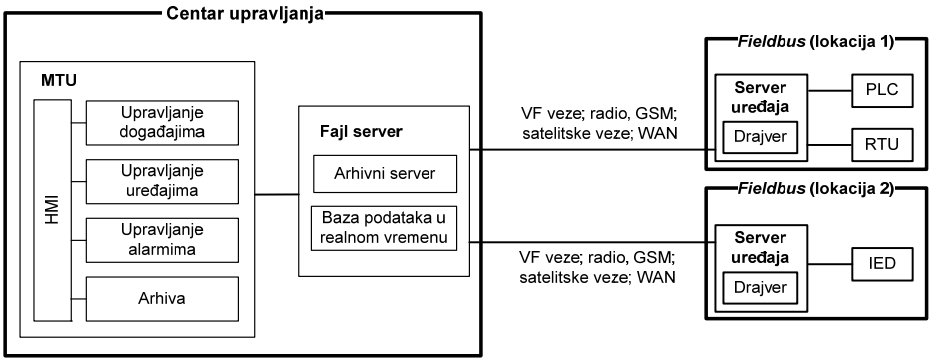
Poslednjih godina se fokus *cloud* računarstva postepeno premešta od potrošačkih aplikacija ka korporativnim sistemima upravljanja. Migracija aplikacija kao što je SCADA ka *cloud* okruženju atraktivna je za poslovne korisnike zbog potencijalnog smanjenja troškova, skalabilnosti, kao i efikasnog konfigurisanja i održavanja sistema. Zakup i pristup resursima vrši se na zahtev, po ceni koja je znatno niža od kupovine, instalacije i održavanja hardvera i softvera, pri čemu se smanjuje broj tehničkog osoblja.

Cilj ovog rada je da razmotri perspektive realizacije SCADA sistema u *cloud* mreži, uzimajući u obzir potencijalne strategije migracije, izbor servisa, kao i prednosti i rizike.

Rad je organizovan na sledeći način. U drugom poglavlju objašnjen je opšti princip funkcionisanja SCADA sistema, a zatim su razmatrane strategije migracije SCADA sistema ka javnoj, privatnoj ili hibridnoj *cloud* infrastrukturi. Treće poglavlje sadrži analizu c*loud* servisa (infrastruktura, platforma ili softver kao servis) sa stanovišta pogodnosti za SCADA aplikacije. Četvrto poglavlje posvećeno je analizi prednosti i rizika pri implementaciji SCADA sistema u *cloud* okruženju. Peto poglavlje sadrži zaključna razmatranja.

2. Migracija SCADA sistema ka *cloud* okruženju

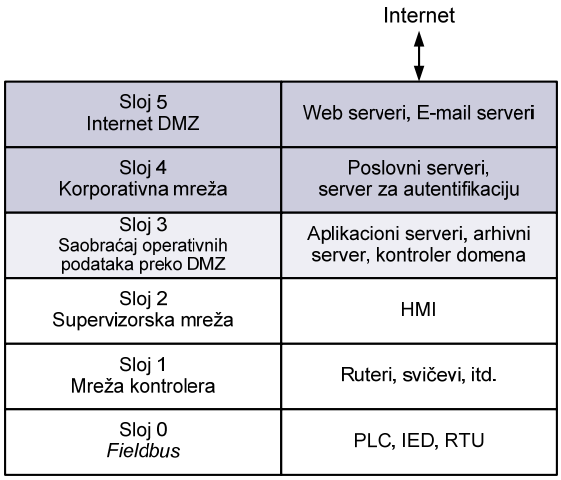
Na slici 1 prikazana je opšta blok šema SCADA sistema. Lokalna mreža u centru upravljanja povezuje SCADA server (*Master Terminal Unit*, MTU), arhivni server, HMI (*Human Machine Interface*) server i konzole, kao i rutere i/ili svičeve za komunikaciju sa daljinskim stanicama. Centar upravljanja prikuplja i analizira informacije od daljinskih stanica (*fieldbus*-ovi na različitim lokacijama), prezentuje ih na HMI i generiše akcije na osnovu detektovanih događaja. Centar upravljanja je odgovoran i za opšte alarme, analizu trendova i generisanje izveštaja. U podsistemu daljinskih telemetrijskih jedinica (*Remote Terminal Units*, RTUs), programabilnih logičkih kontrolera (*Programmable Logic Controllers*, PLCs) i inteligentnih elektronskih uređaja (*Intelligent Electronic Devices*, IEDs) vrši se lokalna kontrola mernih pretvarača i nadzor senzora. Komunikacioni podsistem povezuje centar upravljanja sa podsistemom daljinskih stanica i omogućuje operateru daljinski pristup *fieldbus*-ovima za potrebe dijagnostike i otklanjanja otkaza.



Slika 1. Opšta blok šema SCADA sistema

Za komunikaciju se koriste standardni ili namenski protokoli, preko veza tipa tačka-tačka ili širokopojasne IP-bazirane mreže. Postoji veći broj standardnih i specijalizovanih SCADA komunikacionih protokola među kojima su najrasprostranjeniji Modbus, DNP3 (*Distributed Network Protocol*), IEC protokoli serije 60870-5 i IEC standard 61850 namenjen za transformatorske stanice u električnoj mreži. Većina protokola projektovana je ili prilagođena za rad u TCP/IP mreži. Pored toga, najveći broj savremenih *fieldbus* protokola zasnovan je na Eternet tehnologiji. Sistematizovan pregled SCADA protokola može se pronaći u literaturi [1], [2].

Industrijski sistemi daljinskog upravljanja karakterišu se slojevitom i funkcionalno odvojenom hijerarhijom sa različitim protokolima i fizičkim standardima [1], [3]. Slojevita hijerarhija SCADA sistema definiše se u skladu sa međusobnom vezom njegovih komponenata, kao i načinom povezivanja sa eksternim mrežama, kao što je ilustrovano na slici 2. Najniži sloj (sloj 0) predstavlja fizičke uređaje, koji su u direktnoj interakciji sa fizičkim hardverom, a međusobno su povezani preko *fieldbus*-a. Sloj 1 se sastoji od kontrolera, koji procesiraju signale sa *field* uređaja i generišu odgovarajuće komande za te uređaje. Rezultati procesiranja se prosleđuju sloju 2 na dalju analizu i kontrolu odziva. Sloj 3 tipično predstavlja demilitarizovanu zonu (DMZ) u kojoj su smešteni aplikacioni serveri, arhivni server i kontroleri domena. Viši slojevi odgovaraju korporativnoj IT mreži, koja je povezana na Internet.



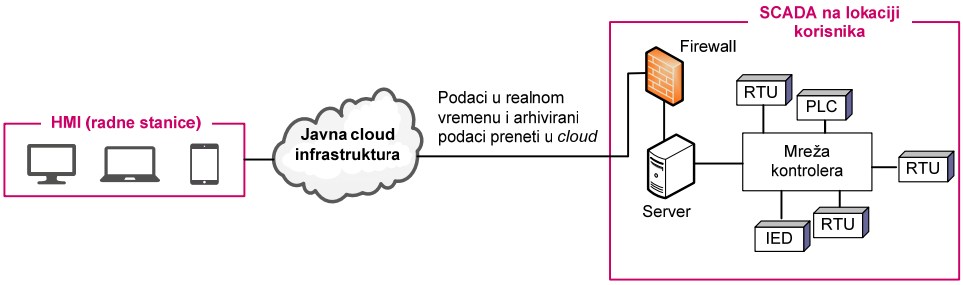
Slika 2. Slojevita struktura SCADA sistema

Pri razmatranju migracije SCADA sistema ka *cloud* okruženju treba imati u vidu da ta infrastruktura može biti javna, privatna i hibridna. Javnu *cloud* infrastrukturu poseduje provajder koji prodaje servise poslovnim i rezidencijalnim korisnicima. Privatnu *cloud* infrastrukturu poseduje ili zakupljuje jedan poslovni korisnik. Takvom infrastrukturom upravlja korisnik ili treća strana, a može biti smeštena na lokaciji korisnika ili na nekoj drugoj lokaciji. Hibridna *cloud* infrastruktura predstavlja kombinaciju privatne i javne infrastrukture, koje ostaju nezavisne celine povezane standardnom ili specijalizovanom tehnologijom koja omogućuje prenosivost podataka i aplikacija.

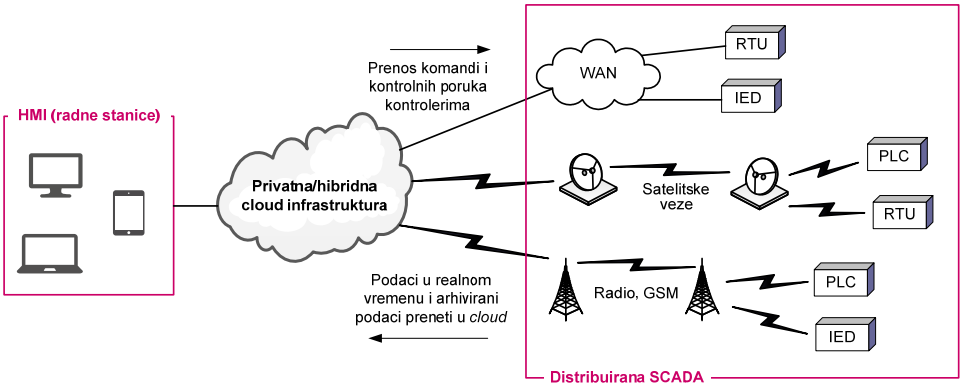
Cloud računarstvo pruža podršku SCADA aplikacijama na dva načina [4]:

1. SCADA aplikacija se izvršava na lokaciji poslovnog korisnika (kompanije, preduzeća i dr.), direktno je povezana na kontrolnu mrežu i šalje informacije u *cloud*, u kome se one mogu čuvati i distribuirati, ili
2. SCADA aplikacija se u potpunosti izvršava u *cloud* okruženju, a daljinski se povezuje na kontrolnu mrežu.

Prvi metod se znatno više koristi, a ilustrovan je na slici 3. Kontrolne funkcije SCADA aplikacije su potpuno izolovane u mreži kontrolera. Sa druge strane, SCADA aplikacija povezana je na *cloud* servise koji omogućuju vizuelizaciju procesa, izveštaje i pristup udaljenih korisnika. Takve aplikacije se obično implementiraju korišćenjem javne *cloud* infrastrukture.



Slika 3. Javna cloud infrastruktura u kojoj SCADA sistem funkcioniše na lokaciji poslovnog korisnika i šalje podatke preko cloud-a



Slika 4. Privatna ili hibridna cloud infrastruktura u kojoj su kontroleri povezani WAN linkovima na SCADA aplikaciju koja se izvršava u cloud-u

Implementacija ilustrovana na slici 4 pogodna je za distribuirane SCADA aplikacije. Kontroleri su povezani preko WAN linkova sa SCADA aplikacijom koja se izvršava u *cloud* okruženju. Takve aplikacije obično se implementiraju u privatnim ili hibridnim *cloud* arhitekturama.

3. Izbor servisa

Servisi dostupni u *cloud* računarstvu mogu se svrstati u sledeće tri kategorije:

1. Infrastruktura kao servis (*Infrastructure as a Service*, IaaS),
2. Platforma kao servis (*Platform as a Service*, PaaS) i
3. Softver kao servis (*Software as a Service*, SaaS).

IaaS je najrazvijeniji i najrasprostranjeniji model servisa, koji omogućuje korisnicima da instaliraju i izvršavaju gotov SCADA softverski proizvod (*off-the-shelf*) kao što bi to činili na sopstvenoj IT infrastrukturi. IaaS pruža usluge virtuelnih servera, memorijskih kapaciteta i drugih fundamentalnih računarskih resursa, na zahtev korisnika. Korisnici plaćaju uslugu korišćenja kapaciteta i mogu, po potrebi, zakupiti dodatne kapacitete. Iako ne upravljaju *cloud* infrastrukturom, korisnici zadržavaju kontrolu nad operativnim sistemima, memorijskim kapacitetima, instaliranim aplikacijama i mogu da selektuju mrežne komponente kao što je *firewall*.

PaaS je skup alata za razvoj softvera, dostupnih u *cloud* infrastrukturi, za kreiranje aplikacija koje se izvršavaju preko Interneta. Korisnici nemaju mogućnost upravljanja *cloud* infrastrukturom, ali kontrolišu aplikacije koje su instalirali, kao i konfiguraciju okruženja. PaaS je pogodan za korisnike koji sami razvijaju SCADA softver na bazi gotovih razvojnih i izvršnih platformi.

SaaS omogućuje korisnicima da koriste aplikacije provajdera koje se izvršavaju u *cloud* infrastrukturi, od različitih klijentskih uređaja do klijentskih interfejsa kao što su pretraživači Weba. Korisnici nemaju mogućnost upravljanja *cloud* infrastrukturom, već samo plaćaju uslugu korišćenja aplikacije. Proizvođači opreme relativno sporo usvajaju SaaS model za aplikacije u jezgru SCADA sistema. Znatno je uobičajenije da se samo pojedine komponente i funkcije SCADA aplikacije, kao što su vizuelizacija i arhivirani izveštaji, realizuju kao SaaS.

Sa stanovišta izbora servisa postoje tri scenarija migracije SCADA sistema u *cloud* okruženje. Prvi scenario (*re-hosting*) je najbrži i najjednostavniji, a pretpostavlja instalaciju postojeće SCADA aplikacije u *cloud* okruženje i zasniva se na IaaS servisu. To je prvi korak u postepenoj migraciji, koji omogućuje da se izvrši analiza i, po potrebi, prilagodi aplikacija, u nekoliko iteracija.

Drugi i treći scenario pretpostavljaju reinženjering u cilju boljeg iskorišćenja prednosti *cloud* računarstva, prvenstveno poboljšanja skalabilnosti i pouzdanosti. To može biti jednostavna modifikacija nekih svojstava (*refactoring*). Primer je implementacija funkcija kontrole resursa, koja omogućuje dodavanje novih resursa kada se aplikacija intenzivno koristi ili oslobađanje resursa koji nisu potrebni. Alternativno se mogu zahtevati veće modifikacije u jezgru aplikacije (*revising*). Primer je korišćenje PaaS baze podataka da se aplikacija izmeni tako da je moguće ponuditi zakup više SaaS servisa. Povećanje broja SaaS ponuda uslovljava zamenu postojeće SCADA aplikacije SaaS rešenjem zasnovanim na *cloud* računarstvu.

Eksperimentalna studija o migraciji odabranog SCADA sistema u IaaS *cloud* okruženje prikazana je u [5]. Imajući u vidu da su za prilagođavanje *cloud* okruženju neophodne određene modifikacije softvera, analizirane su SCADA aplikacije sa slobodno dostupnim izvornim programima, kao što su TANGO, EPICS, Eclipse SCADA i Indigo SCADA. Osnovne karakteristike ovih sistema prikazane su u tabeli 1.

Zatim je korišćena kombinacija *re-hosting* pristupa i testiranja performansi u cilju implementacije Eclipse SCADA softvera u NeCTAR *cloud*[1] (akademska *cloud* mreža u Australiji).

Rezultati testiranja performansi pokazali su da kašnjenje koje unose komponente SCADA sistema u *cloud*-u nije ograničavajući faktor. Izmerena vremena odziva su u opsegu od nekoliko stotina milisekundi do sekunde. Međutim, uočeni su problemi sa

[1] https://nectar.org.au/research-cloud/

polling protokolima kao što je Modbus TCP, koji se zasnivaju na pojedinačnom prozivanju udaljenih stanica. Primena komunikacionih protokola vođenih događajima (*event-driven*) je efikasnija, jer se tako smanjuje intenzitet saobraćaja. Ako to nije moguće, rešenje je da veći broj servera daljinski opslužuje *fieldbus*-ove.

Tabela 1. Karakteristike SCADA sistema sa slobodno dostupnim izvornim programima

Naziv sistema	**Projekat/ proizvođač**	**Tip proizvoda**	**Fieldbus**	**TCP/IP**	**Daljinsko upravljanje**
TANGO[2]	European Synchrotron	Softverski alat	S7, Profibus	Modbus	–
EPICS[3]	Argonne National Laboratory	Gotov proizvod	S7, Profibus	Modbus, Eternet	–
Eclipse SCADA[4]	IoT Industry Working Group	Softverski alat	S7	Modbus	–
Indigo SCADA[5]	Enscada	Gotov proizvod	–	Modbus, RFC1006	DNP3, IEC104, IEC61850

4. Prednosti i rizici pri realizaciji SCADA sistema u *cloud* okruženju

Realizacija SCADA aplikacija u *cloud* okruženju atraktivna je za korisnike prvenstveno zbog unapređenja poslovanja. U nastavku su navedene osnovne prednosti *cloud* računarstva koje motivišu korisnike da izvrše migraciju svojih SCADA sistema [6].

- Zakup i pristup resursima vrši se na zahtev, po ceni koja je znatno niža od kupovine, instalacije i održavanja hardvera i softvera.
- Servis je skalabilan zato što, u slučaju proširenja, nema potrebe za kupovinom i instalacijom farmi servera, baza podataka, Web servera i dr. Lako se može zakupiti dodatni prostor na virtuelnom *cloud* serveru, bez potrebe za instalacijom i održavanjem dodatnog hardvera.
- Smanjuje se broj tehničkog osoblja potrebnog za održavanje IT resursa.
- Informacijama smeštenim na *cloud* serveru može se pristupiti sa bilo kog mesta.
- S obzirom na jednostavan pristup informacijama, saradnja na projektima je lakša i efikasnija.
- Krajnje je jednostavno ažuriranje postojećih i instaliranje novih aplikacija.

Tri glavna faktora rizika za SCADA sisteme u *cloud* okruženju su:

- Bezbednost informacija;
- Performanse sistema;
- Raspoloživost i pouzdanost.

[2] http://www.tango-controls.org/
[3] http://www.aps.anl.gov/epics/
[4] https://www.eclipse.org/eclipsescada/
[5] http://sourceforge.net/projects/indigoscada/

Bezbednosni rizik

Za razliku od javnih i korporativnih informacionih sistema, u kojima je bezbednost informacija i infrastrukture dostigla određeni nivo zrelosti, u industrijskim sistemima ne mogu se pravolinijski uvesti ista rešenja, već su u većini slučajeva potrebna nova rešenja zaštite koja su prilagođena kontrolnom okruženju. Problem bezbednosti sistema koji kontinuirano radi u realnom vremenu zahteva sveobuhvatnu analizu i holističko razumevanje zaštite mreže, teorije upravljanja i fizičkih sistema.

Važnost zaštite kritične infrastrukture ogleda se i u intenzivnim naporima organizacija za standarde da usvoje preporuke i smernice za poboljšanje bezbednosti industrijskih sistema. Relevantni standardi i preporuke obuhvataju opšte IT standarde o bezbednosti, zajedničke standarde i uputstva za zaštitu SCADA i industrijskih sistema daljinskog upravljanja, kao i specifične direktive koje se odnose na pojedine industrijske sektore. Detaljan pregled bezbednosnih standarda i preporuka za SCADA sisteme može se pronaći u literaturi [2], [7].

Upravljanje bezbednosnim rizikom obuhvata analizu rizika, metodologiju procene rizika, izbor mehanizama zaštite i donošenje odluke o implementaciji odgovarajućih mehanizama. Za sprovođenje analize rizika važno je da se prepoznaju, procene i definišu: imovina, potencijalne pretnje, podložnost napadima, posledice napada i mehanizmi zaštite.

Najvažniji deo procesa upravljanja rizikom je procena rizika, koja je ujedno i najpodložnija greškama. Procena bezbednosnog rizika SCADA sistema obuhvata sledeće korake [7]: (1) karakterizacija sistema kroz identifikaciju imovine i određivanje granica sistema; (2) identifikacija pretnji i osetljivosti na pretnje; (3) analiza postojećih i planiranih kontrolnih aktivnosti; (4) određivanje verovatnoće da bi osetljivost SCADA sistema mogla biti zloupotrebljena; (5) analiza uticaja uspešne pretnje; (6) određivanje nivoa rizika; (7) preporuke za ublažavanje rizika i (8) rezultujuća dokumentacija.

U literaturi se mogu naći različiti pristupi, metodi i alati za procenu bezbednosnog rizika. Rad [8] sadrži prikaz i iscrpnu uporednu analizu 24 metoda za procenu bezbednosnog rizika SCADA sistema. Većina tih metoda je generalno primenljiva i na SCADA sisteme u *cloud* okruženju.

Kada neko privredno preduzeće odluči da izvrši migraciju svog SCADA sistema u *cloud* okruženje, potrebno je da izabere provajdera servisa. Pri oceni zrelosti ponuđenih servisa treba uzeti u obzir ispunjenost sledećih kriterijuma [9]:

- Izolacija informacija koje potiču od različitih aplikacija;
- Utvrđivanje nivoa kontrole koju korisnici imaju nad promenama infrastrukture provajdera;
- Kriptozaštita informacija;
- Automatska distribucija dodataka (*patches*) za ažuriranje softvera;
- Redovno i vanredno izveštavanje za potrebe poslovanja;
- Kontinuiran nadzor koji obuhvata procenu efikasnosti bezbednosnih mehanizama, u približno realnom vremenu;
- Mogućnost formiranja i analize log fajlova, detekcije napada u realnom vremenu, odziva na detektovane napade i analize događaja, incidenata, sumnjivih aktivnosti i anomalija;
- Otklanjanje problema, koje obuhvata trenutne korekcije u slučaju identifikacije osetljivosti sistema;

- Pouzdan i kvalitetan korisnički servis.

Najefikasniji način za sigurno sprovođenje zaštite SCADA sistema u *cloud* okruženju je uspostavljanje precizno definisanih sporazuma o nivou servisa koji pokrivaju prethodno navedene kriterijume. Slično istraživanje, koje se odnosilo na poslovne IT sisteme, ukazalo je na značaj uvođenja sporazuma o nivou servisa u kontekstu SaaS i korišćenja otvorenih i slobodno dostupnih softverskih paketa [10]. Uzimajući u obzir procenjeni rizik, opravdano je povećanje troškova u cilju isporuke bezbednih *cloud* servisa.

Performanse sistema

Većina industrijskih aplikacija postavlja stroge zahteve za kvalitet servisa u pogledu kašnjenja, gubitaka i propusnog opsega. Najstrožiji zahtevi za kašnjenje postavljaju se na slojevima *fieldbus*-a i kontrolne mreže. Vremena odziva su u opsegu od 250 μs do 1 ms, a za manje zahtevne procese u opsegu od 1 ms do 10 ms [1]. Viši slojevi imaju progresivno blaže zahteve za kašnjenje, tipično do 1 sekunde.

Korišćenjem javnih *cloud* servisa povećava se rizik da ti zahtevi ne budu ispunjeni, zbog toga što korisnik nema mogućnost kontrole performansi mreže. Posebno je nepovoljno povećano i nepredvidljivo kašnjenje, koje može da blokira rad SCADA sistema u realnom vremenu.

Pre migracije SCADA sistema u *cloud* okruženje potrebno je odgovoriti na sledeća pitanja:

- Kakve su posledice promenljivog kvaliteta servisa na industrijski proces koji kontroliše konkretan SCADA sistem?
- Kakav je uticaj povećanja kašnjenja i varijacije kašnjenja na SCADA sistem?
- Koja je gornja prihvatljiva granica kašnjenja u pojedinim delovima sistema? Na primer, povećanje kašnjenja ne mora da bude kritično u slojevima sistema koji se bave nadzorom i izveštavanjem.

Raspoloživost i pouzdanost

Problem raspoloživosti i pouzdanosti prisutan je kod svakog sistema u *cloud* mreži. Serveri su smešteni na nepoznatim lokacijama kojima korisnik ne može da pristupi. Podaci SCADA sistema sadrže rezultate nadzora i upravljanja industrijskim procesom u realnom vremenu, zbog čega gubitak funkcionalnosti čak i u trajanju od nekoliko sekundi može da izazove ozbiljne posledice na industrijski proces. Na primer, prema preporuci međunarodne organizacije CIGRÉ[6], raspoloživost SCADA sistema u elektroprivredi treba da bude bolja od 99,98% [11].

Treba imati u vidu da su obaveze definisane sporazumom o nivou servisa zasnovane na prosečnim vrednostima mera performansi u velikoj i kompleksnoj mreži. Drugim rečima, stvarno iskustvo korisnika može se značajno razlikovati od vrednosti definisanih klauzulama ugovora.

---

[6] Međunarodni savet za velike električne sisteme *(Conseil International des Grands Réseaux Électriques)*

Zbog toga je, pre migracije SCADA sistema u *cloud* okruženje, potrebno odgovoriti na sledeća pitanja:

- Kakve su posledice otkaza sistema u trajanju od nekoliko minuta?
- Kakve su posledice otkaza sistema u trajanju od nekoliko časova?
- Da li će, u slučaju otkaza sistema, biti izgubljeni važni podaci? Preventivno, neophodno je lokalno čuvanje (*back-up*) svih važnih informacija.

5. Zaključak

Migracija SCADA aplikacija u *cloud* okruženje je relativno nova poslovna strategija koja zahteva detaljnu analizu i pažljivu procenu odnosa prednosti i rizika. Iako primena *cloud* servisa neosporno doprinosi smanjenju troškova i poboljšanju efikasnosti poslovanja, činjenica da su SCADA sistemi deo kritične infrastrukture uslovljava postepen pristup zbog strogih zahteva za bezbednost i kvalitet servisa.

Ako se koriste javni *cloud* servisi, preporučljivo je da kontrolne funkcije SCADA aplikacije ostanu izolovane u mreži kontrolera. *Cloud* servisi se mogu koristiti za supervizorske funkcije (vizuelizacija procesa, izveštaji) i pristup udaljenih korisnika. Kada je reč o izboru servisa, najrasprostranjeniji servis je IaaS, koji zahteva samo *re-hosting* postojećih aplikacija, a korisnik zadržava kontrolu nad instaliranim aplikacijama i računarskim resursima. Bezbednosni rizik može se ublažiti preciznim definisanjem sporazuma o nivou servisa.

U privatnim i hibridnim mrežama, distribuirana SCADA aplikacija se može izvršavati u *cloud*-u, pod uslovom da mreža zadovoljava zahteve za kvalitet servisa, prvenstveno u pogledu vremena odziva i raspoloživosti. Veoma je značajno pravljenje kopija i čuvanje vitalnih podataka na lokalnim serverima.

Zahvalnica. Rad je finansiran od strane Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije (projekti tehnološkog razvoja TR 32025 i TR 36002).

Literatura

[1] B. Galloway, G. P. Hancke. “Introduction to industrial control networks”, *IEEE Communications Surveys and Tutorials*, vol. 15, no. 2, pp. 860–880, 2013.

[2] J. Gao et al., “SCADA communication and security issues”, *Security and Communication Networks*, vol. 7, no. 1, pp. 175–194, 2014.

[3] I. Ahmed et al., “SCADA systems: Challenges for forensic investigators”, *Computer*, vol. 45, no. 12, pp. 44–51, 2012.

[4] L. Combs. (2011). Cloud Computing for SCADA. InduSoft White Paper. [Online]. Available at: http://www.indusoft.com/Documentation/White-Papers/ArtMID/1198/ ArticleID/430/Cloud-Computing-for-SCADA.

[5] P. Church et al., “Migration of a SCADA system to IaaS clouds – a case study”, *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 6, no. 11, pp. 1–12, 2017.

[6] Cloud-Based SCADA Systems: The Benefits & Risks. (2011). Inductive Automation White Paper. [Online]. Available at: https://www.controlglobal.com/assets/ 11WPpdf/ 111202-inductiveautomation-cloud.pdf.

[7] K. Stouffer, J. Falco, K. Scarfone, *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82 Rev. 1, 2013.
[8] Y. Cherdantseva et al., "A review of cyber security risk assessment methods for SCADA systems", *Computers & Security*, vol. 56, pp. 1–27, 2016.
[9] P. D. Howard. (2015). A security checklist for SCADA systems in the cloud. [Online]. Available at: https://gcn.com/articles/2015/06/29/scada-cloud.aspx.
[10] M. Stojanović, V. Aćimović-Raspopović, S. Boštjančič Rakas,"Security management issues for open source ERP in the NGN environment", in *Free and Open Source Enterprise Resource Planning: Systems and Strategies*, R. Atem de Carvalho and B. Johansson (Eds.), pp. 165–181, IGI Global, New York, 2011.
[11] *Integrated Service Networks for Utilities*. CIGRÉ Technical Brochure TB 249, WGD2.07, 2004.

Abstract: *In this paper, we first explain general principles of SCADA system operation, and then evaluate migration strategies of such systems towards public, private or hybrid cloud infrastructure. We further consider selection of the cloud service: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). Finally, special attention is devoted to the analysis of benefits and risks of deploying SCADA applications into the cloud.*

Keywords: *Cloud infrastructure, quality of service, SCADA, security.*

SCADA SYSTEMS IN THE CLOUD ENVIRONMENT

Mirjana Stojanović, Slavica Boštjančič Rakas, Jasna Marković-Petrović